November 2022 · Thorsten Wetzling & Charlotte Dietrich

Disproportionate use of commercially and publicly available data:

Europe's next frontier for intelligence reform?

Stiftung Neue Verantwortung

Think Tank at the Intersection of Technology and Society

Acknowledgements

The authors are solely responsible for the content of this report, and the views expressed herein do not necessarily reflect those of the commentators and reviewers.

We are very grateful for the excellent research and editorial assistance provided by Leo Hennecke, Corbinian Ruckerbauer, and Luisa Seeling as well as for the layout and the visualisations by Alina Siebert (all at SNV Berlin).

We thank the members of the European Intelligence Oversight Network for their important feedback on an earlier discussion paper.

Executive summary

Intelligence services across Europe are increasingly processing commercially available data as well as a broad range of information they deem 'publicly available'. To gain access to such data, they

- purchase data(sets), either ad hoc – when specific information is needed – or on a rolling basis by means of subscription from various data brokers;
- purchase data on the darknet (which may emanate from leaks or stolen customer data);
- buy finished intelligence on the market, without any access to the underlying data (thus outsourcing time and resources for the analysis to private actors);
- purchase from various providers the tools needed for automated analysis of commercially and publicly available data;
- obtain large (bulk) datasets through voluntary submissions of private sector entities, courtesy requests, or gifts;
- purchase or otherwise acquire large datasets through the use of authorised undercover agents or covert human intelligence sources (CHIS).

What these types of access have in common is that they are non-compelled; that is, the entity which provides the intelligence service with access to such data is not obliged by law to do so. This distinguishes these practices from signals intelligence (SIGINT) and computer network exploitation (CNE, commonly known as government hacking), where data held by the private sector can be obtained through compulsion or penetration.

Notably, whereas compelled and direct access have been subject to increasingly dense regulation and oversight in established democracies,[1] governments' purchases of commercially available data or their acquisition and processing of publicly available data still face far fewer legal restrictions and less robust (if any) authorisation and oversight procedures. This deficiency erodes public trust in government and is at odds with the promotion of the rule of law and democracy in Europe. Vague or missing legal restrictions and insufficient oversight may also increase the risk of disproportionate access to personal data without sufficient accountability. In turn, this may increase risks that various rights will be infringed, notably those to privacy, informational self-determination, and freedom of expression.

1 For a comparative overview of good legislative provisions and oversight practice on bulk collection, see intelligence-oversight.org.

While the quantity and easy availability of commercially and publicly available data is profoundly transforming the practice and governance of contemporary intelligence, European lawmakers remain rather oblivious to the gradual paradigm shift and risks involved. To date, regional and European legal frameworks for privacy and data protection are either not applicable or insufficient to rein in these ill-governed practices of national intelligence services. National legal frameworks also lack precision, clarity, and substance: Hardly any European intelligence law currently provides robust legal safeguards, let alone ex ante authorisation and ex post oversight for the various types of data purchases and automated open-source analyses.

Having identified a wide range of governance deficits at both the European and the domestic level, this report shows that the golden era of surveillance is far from over. Indeed, the current labyrinth of public–private co-productions of intelligence and, in particular, non-compelled government access to commercially and publicly available data ought to attract far more legislative attention as well as oversight practice. It should be the next frontier of intelligence reform, and this report aims to provide actionable recommendations, food for thought, and pointers for progress to the pioneers of future intelligence reform.

Table of Contents

Introduction

The rapid spread of web-based services, mobile devices, sensor networks, and the 'internet of things' has caused a sheer inexhaustible availability of data. Many of these data are for sale in a burgeoning data market. Data brokers collect and aggregate information, from both publicly available and private sources, and make these data commercially available. Data brokering, often referred to as the 'biggest industry you've never heard of', comprises over 4,000 companies (Brayne 2020: 23), and the 'global data brokers' market was valued at U.S. $240.3 billion in 2021' (Transparency Market Research 2022). Data brokers cater to the various needs for raw and processed data of their clients. Clients include companies in marketing and risk assessment, but also national security and intelligence services.

In fact, the quantity and quality of commercially and publicly available data are such that they have profoundly transformed the contemporary practice and governance of intelligence and national security. Intelligence services purchase tailored data(sets), either ad hoc – when specific information is needed – or on a rolling basis by means of subscription. In addition, they may obtain large datasets through courtesy requests, voluntary submissions from private sector entities, or gifts as well as in other informal ways involving informants or agents who may refer to unsubstantiated 'emergency instances' (Biddle 2022). Data (leaks) can also be bought on the darknet. Sometimes, intelligence services do not even need to have access to the data as such but can directly buy finished intelligence on the market, thus outsourcing time and resources for the interpretation of raw data. Moreover, they can purchase tools for automated analysis that use commercially and publicly available data. As shown by the innovative work of journalists and civil society actors such as Bellingcat (Higgins 2022), there is huge potential in the systematic exploitation of open-source intelligence (OSINT). Through in-house or purchased cross-system analysis tools, modern intelligence services not only augment their already enormous data repositories with additional data, but also generate new information through richer profiling and pattern analysis that would simply not have been possible solely by means of warrant-based intelligence collection.

This report illuminates how national security agencies' purchases or acquisitions of commercially and publicly available data pose challenges for the democratic and rule-based governance of intelligence. In order to do so, it

- hones in on practices, relevant actors, and the growing relevance of the intelligence services' non-compelled access to personal data and, in so doing, distinguishes this type of access from other modes of intelligence collection (PART I);

- establishes – on the basis of a research sprint and practitioner dialogues with oversight professionals – how current regulatory frameworks, at the regional and national level, do not sufficiently address potential risks and malfeasance related to the intelligence community's (IC) acquisition and use of commercially and publicly available data (PART II);
- discusses ideas and existing practices that lawmakers and oversight practitioners should consider when drawing the contours of a much-needed reform agenda for more rule-based executive conduct in this complex and dynamic field (PART III).

Part I: A paradigm shift in intelligence practice

This section sheds light on various public–private co-productions of intelligence that revolve around the ubiquity of commercially and publicly available data.[2] Arguably, this vast increase in the amount of data used has unleashed a paradigm shift: as Nazareth (2022) observes, 'government analysts are filling the need for intelligence assessments using information sourced from across the internet instead of primarily relying on classified systems or expensive sensors high in the sky or arrayed on the planet'. Naturally, the emergence of this practice poses a wide range of governance questions and concerns that later sections will discuss in further detail. In order to better understand the general direction of travel, the current section focuses first on the practices and players that are relevant to understand the IC's acquisition and processing of commercially and publicly available data.

1. The private sector

The private and public sectors share a long history when it comes to intelligence. As the wide array of electronic espionage programmes that whistleblower Edward Snowden revealed in 2013 have powerfully illustrated, most of the data that are of interest to the intelligence services are held by the private sector. This situation has not changed since then; indeed, this trend has become ever more apparent. What has changed, arguably, is that next to compelling private sector entities to provide government access or directly accessing private sector-held data, contemporary intelligence services increasingly purchase datasets or use broad definitions of publicly available data for automated OSINT to obtain such data. The latter modes of access have not yet drawn enough scrutiny across Europe. Hence, this section first depicts key actors within the private sector and different private sector–public intelligence interactions.

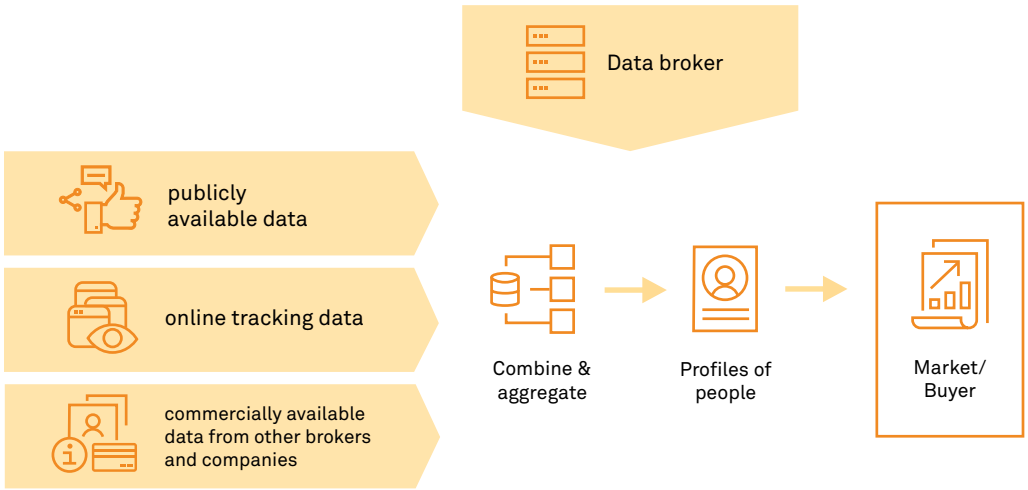
1.1. Data brokers and the quest for (secondary) data

Datasets are mostly sold by data brokers. The Norwegian Consumer Council has defined a data broker as a 'company that processes personal data on consumers, which primarily is not obtained from the consumers themselves but from other companies, in order to sell or license this data – or information derived from it – to further companies' (Forbrukerrådet 2020: 19).

2 Many open questions and governance concerns regarding non-compelled modes of government access to personal data apply equally to the law enforcement and military community. This report focuses solely on the intelligence services, partly because of its limited scope and partly because the legal framework and oversight practice would differ notably, and this, too, would merit further elaboration.

As such, data brokers are 'fundamental actors of surveillance capitalism since they engage in a sort of "information arbitrage": buying, reinterpreting, repackaging, and selling consumer data across contexts' (Reviglio 2022: 11). More specifically, data brokers aggregate, combine, and trade large amounts of data. In order to do so, they use publicly available sources and online tracking data and buy data from other companies, from both the online and offline world (Forbrukerrådet 2020: 19). Data suppliers providing data brokers with data include analytics companies, credit card and social media companies, and many other service providers (Forbrukerrådet 2020: 23). Once they have combined and aggregated the data, brokers can create detailed profiles of people and populations (Twetman and Bergmanis-Korats 2021: 10).

Data brokers' information arbitrage



Data brokers include companies such as Acxiom, Epsilon, CoreLogic, Datalogix, PeekYou, LexisNexis Accurint, Spokeo, Zabasearch, and Thomson Reuters CLEAR (Brayne 2020: 24). Data brokers do not all collect the same data, but usually cater to a specific industry. While most brokers focus on the marketing sector, some specialise in other areas, such as risk assessment, for instance for credit reporting, identity verification, and fraud prevention (Forbrukerrådet 2020: 19). Others primarily offer their services to the public security sector, notably intelligence and law enforcement services but also the military and other security sector agencies, such as customs and immigration services. An investigation of more than 1,500 documents obtained by freedom of information requests by Chris J. Hoofnagle, a privacy scholar in the U.S., has shown that some data brokers have specialised in national security agencies as clients and tailor their data directly to the agencies' needs (Brayne 2020: 25).

1.2. Vendors of cross-system data analysis solutions

Other private sector actors have developed specialised tools for the automated analysis of data from various sources, including commercially available data, social media, and other openly available information. For example, so-called cross-system informational analysis tools enable the joint analysis of different and often very large databases. Broadly speaking, they aim to provide what is often described as an 'x-ray vision' through large datasets. The software can detect connections within seconds that would, if performed manually, have absorbed resources for weeks or months or would simply not have been possible to find. The databases analysed by such tools can range from open-source data to commercially available datasets as well as in-house data that the intelligence services hold themselves. Usually, suppliers of such software are private companies, with Palantir, Accenture, Exterro, and ESRI being just a few examples.

The Dutch intelligence oversight body Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten (CTIVD) recently reported that both the Dutch intelligence services Algemene Inlichtingen- en Veiligheidsdienst (AIVD) and Militaire Inlichtingen- en Veiligheidsdienst (MIVD) have purchased tools from the private sector to perform automated OSINT as well as tools to process commercially available data on targets (CTIVD 2022: 17-19). Such analysis tools help to generate new information by combining and cross-analysing several datasets. They can be particularly important when in-house data are combined with commercially acquired data and OSINT (Wetzling et al. 2021). It is most likely that other security and intelligence agencies throughout Europe, but also fusion centres such as the Belgian National Travel Targeting Center (NTTC), rely substantially on purchased data as well as very broadly defined open-source information.

2. Different intelligence–private sector interactions

As indicated, there are different ways in which the intelligence services can gain access to data held by the private sector, including

- **Compelled access:** when the intelligence services can legally oblige private sector actors, such as internet service providers, to provide access to data, for example data streams in their backbone fibre optic cables;
- **Direct access:** when the intelligence services obtain access to data held by the private sector by means of direct interference with (foreign) information technology (IT) systems or communication networks. Such direct access may occur with or without the private sector's knowledge or involvement. Often, there is no legal process for private sector actors to legally challenge direct access practices in court.

- **Non-compelled access**: when, by contrast, entities holding commercially or publicly available data are not obliged by law to cooperate with the government. Instead, they may provide access voluntarily, such as for financial gains or another incentive.[3]

These access trajectories vary with regard to the degree of external scrutiny involved. The table below illustrates this broad characterisation of access types further.

Access trajectories

Access type	Description	Practice examples
Compelled access	Intelligence community (IC) can legally oblige private sector actors, such as internet service providers, to provide access to data.	→ Foreign communications data from domestic internet exchange services (bulk collection) → Inventory data from platform operators (criminal investigations) → Data disclosures from private sector entities during a state of emergency
Direct access	IC obtains access to data held by the private sector by means of direct interference with (foreign) information technology (IT) systems or communication networks. Such direct access may occur with or without the private sector's knowledge or involvement. Often, there is no legal process for private sector actors to legally challenge direct access practices in court.	→ (Bulk) hacking of (foreign) ISPs → Tapping of high capacity fibre-optic cables which carry internet traffic
Non-compelled access	IC acquires or receives access to commercially available data from a private sector entity, such as a data broker, without a legal requirement to provide access. Instead, private sector actors may provide access voluntarily, such as for financial gains or another incentive.	→ Advertisement intelligence (ADINT), → (Automated) open source intelligence (OSINT) → Social media intelligence (SOCMINT) → Access to such data through specialised analysis tools → Publicly available data

The datasets to which intelligence services gain access by non-compelled means can comprise different types of information. The most common ones, usually sold by data brokers, contain information gathered for advertisement or risk-assessment purposes. These can include location data, personal advertisement identifiers, financial data, device identifiers, browsing history, etc. (Forbrukerrådet 2020).

3 A potential constraint could be the prospect of a favourable tax decision in return for frequent cooperation on non-compelled courtesy requests for data. Another factor could be a company's fear for its reputation if the public learned that it was not cooperating with governments' non-compelled requests regarding data relating to issues such as child sexual abuse.

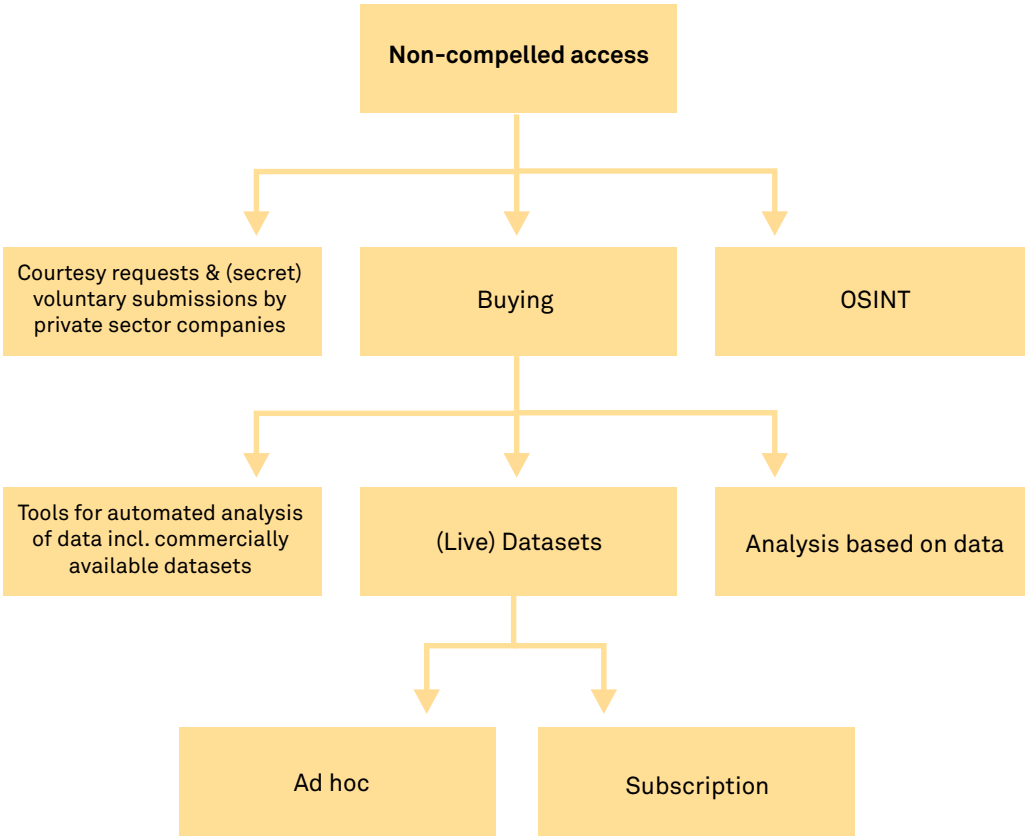
Information in datasets and analysis platforms sometimes also draws on sources from leaked datasets that can be acquired on the darknet.[4] The data can be sold in their raw state or in a processed state.

OSINT may also be included in the category of non-compelled access. OSINT comprises openly accessible data from sources such as the media, social media, and other public data. It has become more difficult to define what constitutes publicly available data since, with digitalisation, all of us leave public traces all the time, whether willingly or unwillingly.

In addition, intelligence agencies may receive access to commercially available data through courtesy requests or voluntary submissions and gifts from private sector entities.

As the following non-exhaustive summary illustrates, non-compelled intelligence services' access to personal data can take various forms.

Modes of non-compelled access



4 In the Netherlands, for instance, bulk datasets were purchased by the Joint SIGINT Cyber Unit (JSCU) on an illegal internet marketplace on the darknet (CTIVD 2017: 12).

The most straightforward form is the purchase of data(sets), either ad hoc when specific information is needed or on a rolling basis by means of subscription.

Outsourcing analysis to the private sector can be a means to indirectly obtain information that is based on commercially available datasets. In this case, intelligence agencies do not necessarily have access to the data as such but directly buy analysis informed by the data, thus outsourcing time- and resource-consuming data interpretation.

It is, moreover, important to note that the private sector does not only provide data, but also plays a crucial role when it comes to profiling and analysis. Intelligence services may thus purchase tools for automated analysis of data contained in both commercially and publicly available datasets (CTIVD 2022).

3. The relevance and risks of commercially and publicly available data

When the many traces that each individual leaves behind in this digitalised world are well combined and processed in cross-system information analysis systems, far more granular light can be shed on nearly every part of a person's personality and behaviour than if a single data source were used. Similarly, key insights about populations as a whole can also be derived from cross-system information analysis. Intelligence services are thus generally keen to run a plurality of data collection modes simultaneously, even if it may lead to over-collection of data.

Yet, by comparison with compelled or direct access, there are also unique advantages of the systematic collection and processing of publicly and commercially available data that may help to explain (and propel) the ongoing paradigm shift. Whereas compelled access to, say, location data of specially protected persons (e.g., journalists, lawyers, priests) requires a warrant and comes with several data-processing requirements in many democracies, data purchases and automated OSINT processing, to date, impose far fewer (if any) of such restrictions on the intelligence services. Non-compelled modes of intelligence collection thus allow them to reach their objectives without having to adhere to lengthy authorisation processes and complex data-processing requirements. Given that warrant regimes and data processing requirements have become far more elaborate and rigorous in recent years for compelled and, gradually also for direct modes of government access, this may render the recourse to non-compelled modes of access even more attractive going forward. What is more, the systematic collection of commercially and publicly available data absorbs less resources and can, depending on the information sought, be more economical than direct or compelled modes of accessing personal data held by the private sector.

Yet, there are also several risks that the intelligence services, lawmakers, and oversight professionals should bear in mind: First, as noted by Zegart, the accuracy and quality of OSINT and purchased data ought to be verified:

> *In a world of cheap satellite imagery, deepfakes, and the weaponization of social media, foreign governments, their proxies, and third party organizations and individuals will all be able to inject convincing, false information and narratives into the public domain at speed and scale. If their goal is to confuse rather than convince, a little deception can go a long way (Zegart 2022: 246).*

While the risk of deception exists for all types of intelligence, it is particularly high when it comes to OSINT and purchased data, where fakes are much easier and cheaper to implement. Additionally, the quality of the data can be bad even without interference from a third party whether by mistake, through systemic biases, or because data collection was poorly executed (Ferguson 2017: 1154) At a minimum, therefore, the services and their political masters, but also their independent overseers, must be sufficiently trained and equipped to verify the accuracy of data obtained through non-compelled modes of access, especially if these data are to be pooled with other sensitive data and then shared with other agencies.

Second, the large-scale collection and subsequent processing of personal data can render data subjects vulnerable to fraud, manipulation, and discrimination (Forbrukerrådet 2020). While it should be alarming enough that intimate data and personality profiles are in the hands of private companies, this situation becomes even more problematic when such data are in the possession of government agencies with executive powers. As Twetman and Bergmanis-Korats point out in a study by the NATO Strategic Communications Centre of Excellence (NATO StratCom COE), the easy accessibility of such detailed data can also constitute a national security risk (Twetman and Bergmanis-Korats 2021). Alongside risks of manipulation and disinformation campaigns by third countries, such databases could also give out security-relevant information, such as the location data of military personnel, or even provide intimate or compromising information about national security staff, rendering them more vulnerable to espionage and extortion.

Third, and this is the focus of the current report, there are genuine risks that ill-governed and insufficiently overseen data purchases and automated OSINT practices infringe upon the rights to privacy, informational self-determination, and freedom of expression and therefore need to be regulated and controlled more rigorously going forward.

4. Non-compelled access to commercially available data in practice

Before assessing the aptness of different regulatory frameworks and oversight practices in regard to the many challenges and risks of non-compelled government access to data held by the private sector, we briefly highlight one such practice with a view to providing a more tangible illustration of the substantial governance challenge and pressing need for future legislative action.[5]

Meet FOG Data Science and FOG Reveal. According to recent reports by the Electronic Frontier Foundation and Associated Press, FOG Data Science is a private U.S. company that exploits a 'near real-time database of billions of geolocation signals derived from smartphones' and 'sells subscriptions to a service [...] that lets law enforcement look up location data in its database through a website' (Cyphers 2022).[6] Individual users who bought subscriptions to the website and underlying database can perform two different types of searches: 'area searches' and 'device searches'. The former type 'allows law enforcement to draw one or more shapes on a map and specify a time range they would like to search. The service will show a list of all cell-phone location signals (including location, time, and device ID) within the specified area(s) during that time' (ibid). The latter type allows agents to 'specify one or more devices they've identified and a time range, and FOG Reveal will return a list of location signals associated with each device' (ibid).

Importantly, this mixture of broad and specific searches allows users of FOG Reveal to effectuate searches 'that are functionally equivalent to the geofence warrants that are commonly served to Google' (ibid). There is an important difference, however: unlike geofence warrants (a compelled mode of access), FOG Reveal does not require law enforcement, or intelligence agencies, for that matter,[7] to obtain a warrant first.

5 Evidently, choosing only one example is inherently selective. Its purpose is to further illustrate what the security services' purchases of tools and datasets might look like in practice. Readers should know, however, that since the widespread nature of law enforcement purchase of the services offered by FOG Data Science was revealed (Cyphers 2022; Burke and Dearen 2022), many other stories on other companies and tools have appeared, which are equally revealing (notably, Cox 2022).

6 Apparently, 'the smartphone signals in Fog's database include latitude, longitude, timestamp, and a device ID' (Cyphers 2022). The company is also reported to 'access historical data reaching back to at least June 2017' (ibid).

7 In the reported case of FOG Reveal, the focus is on state law enforcement agencies. However, the company states further 'use cases' that range 'from the dramatic ("Human Trafficking," "Terrorism Investigations," "Counter-Intelligence") to the more mundane ("Drug Investigations," "Soft Target Protection")' (Cyphers 2022). Consequently, the authors finds that FOG Reveal 'seems to be aimed at both local law enforcement and at intelligence/homeland security agencies' (ibid).

As regards the origins of the data that FOG Reveal uses, they originate

> *from third-party apps on smartphones. Apps that have permission to collect a user's location can share that data with third-party advertisers or data brokers in exchange for extra ad revenue or direct payouts. Downstream, data brokers collect data from many different apps, then link the different data streams to individual devices using advertising identifiers. Data brokers often sell to other data brokers, obfuscating the sources of their data and the terms on which it was collected. Eventually, huge quantities of data can end up in the hands of actors with the power of state violence: police, intelligence agencies, and the military. As one possible source of the data, the authors refer to "unstructured geo-spatial data emanating from open apps (Starbucks, Waze, etc.)" (ibid).*

This particular case, the use of *FOG Data Science* and *FOG Reveal* by U.S. law enforcement agencies (LEAs), shows how huge quantities of often highly sensitive data, that would normally require a warrant, are being transferred to executive agencies via private companies without appropriate safeguards. As indicated, this is just one of several such examples, and the next section investigates whether European regulatory frameworks and oversight practice are currently fit for purpose or need to be reformed to better protect our democracies from such risks and illiberal security practices.

Part II: Policy and governance challenges

As indicated in the previous section, many investigative journalists are currently focusing on the burgeoning data market in the U.S. and the many ways in which U.S. law enforcement and the IC either purchase finished intelligence or subscribe to various data analysis services or datasets sold to them by a wide range of different data brokers. Investigative reporting by Motherboard and Vice has revealed, for example, that the U.S. military had acquired location data and other sensitive data from – amongst other apps – a Muslim prayer app and a Muslim dating app.[8] These revelations have, in turn, triggered various new reform proposals in the U.S.[9]

In Europe, by contrast, there has been far less discussion of this sensitive issue. One reason for this, presumably, has to do with the fact that, by comparison, the European Union (EU) has enacted more privacy-protecting regulations than the U.S. These include, notably, the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), and a slew of other, more recently adopted, frameworks, such as the Digital Services Act (DSA) and the EU Data Act. In addition, the Council of Europe has updated its Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108).

Thus, before any further analysis is carried out, the question ought to be raised of whether poorly regulated and insufficiently overseen non-compelled access to personal data is only a genuine policy problem in the U.S. Put differently, are the citizens of the EU less exposed to these risks thanks to the GDPR and corresponding regulatory frameworks at the national level? And, if so, is this enough to alleviate concerns and the need for reform?

This section shows where and how European and national legal frameworks and oversight practices are currently challenged and whether they are fit for purpose.

1. A 'whole of privacy approach' to public–private co-productions of intelligence

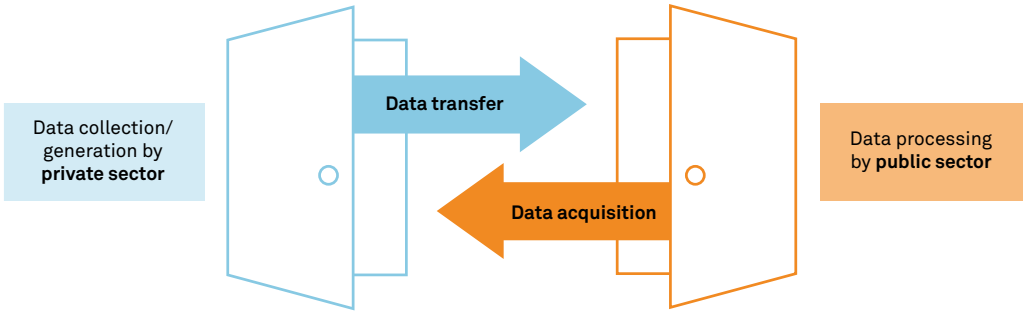
Arguably, securing rule-based and proportionate government conduct in a policy field that involves various modes of public–private interaction requires a multi-layered accountability approach that should focus on both the public and the private sector.

8 See (Cox 2020).

9 Notably, this includes the Fourth Amendment Is Not For Sale Act, introduced by Senator Wyden, and a range of ongoing discussions and (as well as lobbying attempts by data brokers) concerning the American Data Privacy And Protection Act (ADPPA), see (Ng 2022). In addition, the U.S. Privacy and Civil Liberties Oversight Board (PCLOB) is currently reviewing the FBI's activities with regards to commercially available and open-source data (PCLOB 2022).

Such an approach is needed because what ought to be protected or safeguarded does not rest with one actor type alone. Instead, lawmakers and overseers need to work on several accountability construction sites simultaneously. The following illustration further explains the various dimensions, accountability layers, and need for these layers to be in sync.

Networked web of accountability



private sector → public sector	public sector → private sector
In order to get a better grip on the burgeoning data market itself, that is, platforms, app providers, data brokers, etc, the first layer – accountability for the private sector – has to make sure that **rules are in place in regard to:**	As regards the second layer – accountability for the public sector's engagement and subsequent use of private sector products and data – **rules need to be in place and enforced in regard to:**
→ what data can lawfully be generated/collected; → what data can be transferred to third parties; → what data protection regimes are in place and what role they play when it comes to selling data-driven services to the government; → the enforcement and independent verification of the adherence to these rules; – specifically: accountability for data brokers and vendors of analytical software for the analysis of commercially and publicly available information.	→ what data can/cannot be bought/ systematically collected; → what criteria and legal safeguards need to be spelled out in writing so as to sufficiently regulate these practices; → what authorisation process/ex post oversight systems ought to be in place as well as reporting obligations for review bodies; → what general as well as enhanced transparency requirements should be in use so as to give lawmakers and the general public a regular update on the scope and relevance of this practice.

Furthermore, the individual accountability layers need to be more aligned and in sync to prevent disproportionate access and abuse. Inspiration can be taken from the 'double-door model' developed by the German Federal Constitutional Court (Bundesverfassungsgericht; hereafter BVerfG) in 2012 which requires separate regulations for inter-agency data transfers for both the agency requesting information and that providing it. Transposed to government–private sector relations, such a 'double-door model' underlines that accountability mechanisms and safeguards need to exist for both actors in, or both 'sides' of, the data transfer that takes place.

Such a networked web of accountability layers is not yet in existence in the U.S. As we shall see in the next two sections, the situation in Europe may be better, but it is by no means sufficient to meet the various challenges of the paradigm shift in intelligence practice discussed in Section I of this report.

2. Loopholes in European data and privacy protection

As a first part of the analysis, this section subjects relevant European data and privacy protection frameworks and their enforcement record to further scrutiny. The analysis begins with pertinent elements within the EU and Council of Europe regulatory landscape and their potential effect on the governance of national security by Member States. While, naturally, the national level still has far more weight in the national security domain, European data protection and privacy standards are fast evolving and, thanks to the recent jurisprudence of the European Court of Justice (CJEU), national security governance is no longer entirely off-limits for harmonisation at the regional level. In regard to the 'whole of privacy approach' that was outlined in the previous section, in particular, European privacy regulations are increasingly important, as they focus on regulation of the private sector before data are transferred to government agencies.

This is not to say, however, that the relevant regulatory frameworks of the EU and the Council of Europe have a firm grip on the practice of non-compelled government access to personal data held by the private sector. The situation is, in fact, quite the contrary, as shown by the following discussion, which focuses first on the GDPR and the LED before turning to the European Charter of Fundamental Rights and the Council of Europe's modernised Convention 108.

2.1. The General Data Protection Regulation (GDPR)

The GDPR came into effect in 2018. Its Article 5 lays out the general principles according to which personal data must be collected and processed: lawfulness, fairness, and transparency; purpose limitation; data minimisation (i.e., acquiring more data than necessary is unlawful); accuracy; storage limitation; and integrity and confidentiality. Clear opt-out rights for data subjects and the introduction of a risk-based approach to compliance increase the accountability of data controllers and strengthen the enforcement of data subject rights (Rieke et al. 2016: 22).[10] The higher the risk for negative impacts on the data subject's rights, freedoms, and interests, the stricter the compliance mechanisms applying to data processing will be. The level of risk depends on which data are collected, how and by whom they are processed, and the severity and likelihood of negative impacts. The level of compliance mechanisms is determined by the accountability obligations which apply to the controller. In addition, the GDPR adds purpose limitation as a significant safeguard, which forbids data from being collected and sold for a purpose not defined at the moment of collection (ibid.).

Prima facie, EU legislation thus imposes both ex ante and ex post control on data controllers: 'when collecting data, the controller must inform the consumer of the controller's identity and the reasons why the data are processed', which, together with data minimisation, constitutes ex ante control on the data controller (Reviglio 2022: 9). The legislation ensures ex post control by

> *enabling consumers to access, monitor, and correct personal data post-processing (and giving them) the ability to challenge data processing, such as the right to erasure (also referred to as the right to be forgotten, GDPR art. 17), the right to data portability, and the right not to be subject to a decision based solely on automated processing and profiling (ibid.).*

While 'certain controls are subject to commercial flexibility exceptions, which may undermine privacy protection', the EU framework 'provides strong sanctions and compensation that incentivise companies to take regulation seriously' (ibid.)

The GDPR applies to both the private and the public sector. It does not, however, apply to activities that fall outside the scope of EU law, which includes substantial parts of the national security remit as well as processing activities carried out for the purposes covered by the LED (see below). Based on Article 23(1) GDPR, EU or Member State law may restrict the GDPR for the purpose of national security.

10 The risk-based approach to compliance requires accountability mechanisms adjusted to the risk level of data processing.

The GDPR further allows data brokers to share personal data with law enforcement if they have a lawful basis under Article 6. Such a lawful basis exists when processing is necessary to protect the vital interests of a natural person under Article 6(1)(d) or for the performance of a task carried out in the public interest (Article 6(1)(e). However, data brokers collecting and processing data for commercial purposes would still need to satisfy the purpose limitation principle when *selling* such data to national security agencies, as such a transaction would constitute a new purpose; thus, the GDPR is applicable to data collected by data brokers when such data are sold to the public sector even within the national security remit.

Thus, at least partially, this observation answers the question with regard to the difference between the EU and non-GDPR countries such as the U.S. The former has a much stronger de jure net of safeguards, which makes it costlier and riskier for data brokers to cater to European intelligence services. Generally, the GDPR has been an important achievement for the promotion of data subject rights. Due to the various provisions mentioned, the GDPR has – de jure – substantially limited what data can legally be collected and how.

By and large, one might therefore expect that much less sensitive data are being collected and processed by data brokers in the EU and, in turn, sold to national security agencies in countries subject to the GDPR. Reportedly, available data are indeed scarcer, and EU data are more expensive (Twetman and Bergmanis-Korats 2021).

It might be presumed that these important de jure safeguards also have a notable de facto impact on the scope and breadth of the non-compelled private–public sector interactions described in Part I of this report. Unfortunately, the de facto effect of the GDPR on data purchases by national security establishments is not so easy to establish. While some scholars argue that 'the GDPR has had a major impact and further harmonized the EU data protection landscape, including data brokers' (Chih-Liang 2018: 6), they also point out that 'the possibility of exceptions, divergent interpretations, legal cultures, and national laws that lack harmonization remains of concern' (Chih-Liang 2018: 6). To date, 'no authoritative report has been published about how EU data protection law applies to data brokers' (Chih-Liang 2018: 6). What is more, 'no coordinated enforcement against data brokers has occurred in the European Union. At the EU level, the Article 29 Working Party, which comprises representatives from all EU Data Protection Authorities (DPAs), has yet to specifically address applying the existing rules to data brokers' (ibid).

Indeed, compliance with and enforcement of the GDPR remain highly unsatisfactory. Most data brokers do not have the capacities or entrepreneurial will to ensure that contractual obligations on the lawful use of data are respected (Twetman and Bergmanis-Korats 2021: 14). Hence, once data have been sold, it is even more difficult to ensure compliance with the GDPR. An investigation by the NATO StratCom COE has shown that the European adtech company from which they purchased data did perform some vetting of the client before selling the datasets in order to ensure the legitimacy of the client and lawful use of the data. However, this practice is not industry standard, and, as the authors of the report rightfully pointed out, there are easy workarounds for such screenings, such as creating shell firms (Twetman and Bergmanis-Korats 2021: 14-15). A 2020 report by the Norwegian Consumer Council has shown, for instance, that major apps, such as Grindr, a dating app mostly catering to gay men, or MyDays, a period tracking app, are collecting and sharing extremely sensitive data while being systematically non-compliant with the GDPR (Forbrukerrådet 2020). The report reveals how consumers are pervasively tracked and profiled online and have no way of knowing either who is processing their data nor how to oppose such profiling.[11] It concludes that the European adtech industry is systemically non-compliant with the GDPR.

In light of systematic non-compliance within the data market in Europe and the difficulty of actually ensuring lawful use of data once they have been sold, the safeguards of the GDPR are insufficient to guarantee rule-based and proportional conduct when brokers sell datasets to national security agencies. Furthermore, as long as large cross-border cases fall under the remit of under-resourced and more market-oriented national DPAs, such as the Irish DPA, this first-instance one-stop-shop authority for enforcing safeguards union-wide constitutes another weak link. While

> *the GDPR has established a cooperation mechanism for DPAs to resolve cases together … most of them rely on their national procedure to operate within this European system. In practice, this means that DPAs leading on cases sometimes technically cannot share information on their draft decisions or investigations with colleagues (Massé 2022: 4).*

Rightly, Access Now and others thus recommend strengthening the position of the European Data Protection Board (EDPB) when it comes to its direct and early involvement in larger cross-border cases (ibid).

11 The EU's Digital Service Act (DSA) imposes a ban on targeted advertising based on the use of sensitive personal data that includes ethnicity, sexual orientation, and religious and political beliefs. It is likely to diminish the amount of such highly sensitive commercially available data on the market.

Given the burgeoning market for personal data outside and inside Europe, European intelligence agencies can purchase datasets once they are on the market, irrespective of whether or not the data were collected in a GDPR-compliant manner. Due to the secrecy involved, there is little actual proof available to the public documenting where and how national security and intelligence agencies in Europe are purchasing commercially available data. Still, as indicated in the CTIVD report mentioned earlier, there are clear indications and some reported instances that demand far greater scrutiny.

Another important aspect to consider is that rapid developments in IT can now call into question some underlying definitions in data protection. For instance, the GDPR only applies to personal data, but the concept of 'personal data' has become increasingly contested in the context of big data.

Article 4 of the GDPR defines personal data as follows:

> *Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Thus, data protection relies on the delimitation between identifiable and anonymous data. Data that were personal can be anonymised. In their anonymised state, they are no longer subject to (the same) data protection regulations (Hornung and Wagner 2019). However, with growing computing capacities and more refined analysis tools, de-anonymisation of data has not only become possible, but increasingly easy and cheap. In an era of big data, anonymisation has therefore become questionable, to say the least, as the vast majority of data can become personal (Boehme-Neßler 2016).

Thus, as regards the impact of the GDPR on intelligence services' non-compelled access to personal data held by the private sector, one can summarise that it has significantly restricted the European data market. Put differently, the enhanced data subject rights of the GDPR substantially limit, at least de jure, the supply of commercially available data that can be acquired for intelligence purposes. The GDPR may also have made European data more expensive by comparison with data from other regions of the world. That said, at least for the data broker–national security agency interaction, the GDPR is an important but by no means sufficient response to a burgeoning data market catering to the interests of the IC. This shortcoming is due to its grave enforcement deficits, the general national security exemption, and a focus on personal data that is problematic in times of evolving big data analysis.

2.2. The EU Law Enforcement Directive (LED)

The LED, often called the small sibling of the GDPR, is the EU's pertinent framework for the processing of data by the police and criminal justice system. Unlike the GDPR, it directly applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data.

A data broker's obligations would thus be dictated by the GDPR, and a law enforcement agency's (LEA) obligations would be determined by the LED. The latter includes several relevant safeguards. For example,

- it requires an adequate legal basis for the processing of data and the use of automated analysis systems (Art 8);
- it demands a strict assessment of necessity and proportionality (Arts 8 and 10) as well as appropriate safeguards (Art 11);
- it demands a concrete authorisation in the law for the processing of data unless the data has been 'manifestly made public' (Art 10).

However, the LED has to be transposed into EU Member State law, and this has not yet happened everywhere. Germany, for instance, has still not comprehensively included the LED in national law. Consequently, the country was recently reprimanded by the European Commission for not yet having 'notified measures transposing the Directive in relation to the activities of the Federal Police' (European Commission 2022). Without a legal basis in national law, national privacy and data protection authorities can lack binding powers to stop non-compliance with the LED (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) 2021). Other EU Member States have also not sufficiently transposed the LED, which also affects the protection of appropriate safeguards.[12]

More importantly for the practices discussed in Part I of this report, the LED is geared towards law enforcement services and rarely, if ever, applies to the practices of intelligence services. This view can be challenged, however. As argued by Saifert and Quintel, 'when national intelligence agencies process data for the purposes of the Directive, they should be viewed as competent authorities under Article 2(1) instead of not being covered by EU law' (Sajfert and Quintel 2017: 4). Clearly, there are many overlaps between police-led intelligence and intelligence-led policing, and not all intelligence data processing should fall outside the scope of the LED just

12 Greece, Finland, and Sweden have received, together with Germany, formal letters of notification for failing to fulfil their notification duties relating to the GDPR and the LED (European Commission 2022).

because a national security agency and not a LEA is involved. In practice, however, the LED offers little de facto orientation for the legality and democratic governance of non-compelled intelligence access to data held by the private sector.[13]

2.3. The European Charter of Fundamental Rights

Given the many exemptions made for intelligence data collection and processing in data protection and privacy frameworks such as the GDPR and the LED, the question thus remains of what role, if any, European regional frameworks play in the governance of private sector–intelligence service interactions in EU Member States.

National governments are keen to remain entirely autonomous in their decision-making when it comes to intelligence. Yet, in an ever-closer EU, it is not set in stone that intelligence will always remain the untouchable bastion of national sovereignty. Indeed, different factors are currently bringing new momentum not only to the longstanding call for more intelligence cooperation, but also to the harmonisation of intelligence governance standards and safeguards among EU Member States.

As regards the former, Russia's war against Ukraine ignited new calls for further intelligence cooperation in Europe at both the international and the supranational level.[14] As regards the *harmonisation* of some intelligence practices and corresponding safeguards among EU Member States, the recent jurisprudence of the CJEU is particularly insightful.[15] More specifically, its recent decisions in the field of metadata retention and national security have, to put it mildly, ruffled feathers in national security and intelligence establishments across Europe. The *Privacy International* case brings up 'retention of telecommunications metadata for national security purposes within the scope of EU law' whereas the *La Quadrature du Net and Others* judgement

> *sets out the limits which apply to state use of the national security exception to the protection of fundamental rights set out in the EU Charter. Read together, and in*

13 See (Drechsler 2020) also on the weaknesses of the LED when it comes to LEAs' data transfers to LEAs in third countries not bound by the LED. The same holds true for information sharing between national intelligence agencies and LEAs in third countries.

14 Naturally, more density in intelligence cooperation would also require revived discussions and action on states' individual responsibilities for the joint governance of intelligence cooperation as well as ways to better ensure independent and robust oversight and accountability for the different modes of intelligence cooperation.

15 Case C-623/17, *Privacy International* v. *Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*, Judgement of the Court of Justice (Grand Chamber) of 6 October 2020, EU:C:2020:790, and Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others* v. *Premier ministre and others*, Judgement of the Court of Justice (Grand Chamber) of 6 October 2020, EU:C:2020:791

> *line with the existing case-law, they constitute a revised EU legal framework within which security services of all Member States must operate and which must be fully respected by both the national and EU legislatures (Mitsilegas et al 2022: 2).*

By contrast, the default position of most national security and intelligence establishments across Europe is a broad understanding of Article 4(2) of the Treaty Establishing the European Union (TEU), which states that 'national security remains the sole responsibility of each Member State'. This, they believe, shields Member States' national security laws and policies from any encroachments through EU law or CJEU jurisprudence. The CJEU, however, does not subscribe to this broad view. Rather, it held in the *La Quadrature du Net and Others* judgement that 'the mere fact that a national measure was taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law' (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, para 99). More specifically, and concerning intelligence services' *compelled access* to metadata held by the private sector, the CJEU 'considers that as soon as a national legislature enacts powers requiring natural or legal persons to cooperate with national security agencies in some way, and such an obligation in some way involves a limitation of a natural or legal person's rights under primary or secondary EU law, then the exclusion in Article 4(2) TEU does not apply' (Cameron 2021: 26).

The quarrel between those favouring a more extensive or restrictive scope for EU law when applied to national security and intelligence is ongoing and intensifying. Future debates on the (partial) harmonisation of national security standards and safeguards in Europe ought to extend their focus to non-compelled intelligence service access to purchased or secondary data. As discussed in Part I of this report, such access also involves instances where a 'natural or legal person cooperat(es) with national security agencies in many different forms, many of which also involve a limitation of a natural or legal person's right under primary or secondary EU law' (Cameron 2021: 26)

At present, we may conclude that while the exact applicability of EU law to Member States' national security and intelligence practice remains contested, the partial harmonisation of EU-wide intelligence governance standards has progressed. It is no longer wishful thinking on the part of a handful of academics but part and parcel of the democratisation of security governance, to which the CJEU contributes significantly.

2.4. Convention 108+

Turning away from the EU and towards the Council of Europe, the modernised Convention 108 might provide further orientation and guidance for the governance of intelligence services' non-compelled access to personal data held by the private sector.[16] This convention applies data protection principles to all processing activities and is the only international legal framework where the entire catalogue of safeguards explicitly extends to cases where the data processing takes place for security and defence purposes. The following are among the important safeguards of the modernised Convention 108:

- 'data processing activities for national security and defense purposes need to be "subject to independent and effective review and supervision under the domestic legislation' (Art. 11.3.);
- the 'processing of genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life,' needs to be subject to safeguards laid down in the law (Art 6);
- legitimate bases under which data can be processed need to be laid down by law (Art 5.2.).

The exceptions for the cases of national security and defence as described in Article 11 of the Convention have, however, been criticised as being far too broad and giving state parties enormous leeway (Wetzling and Dietrich 2021). Most importantly, however, the modernised Convention has not yet been ratified by a majority of European countries, including France, the UK, the Netherlands, and Norway (Council of Europe 2022).

2.5. Summary

This section has shown that non-compelled modes of access to data held by the private sector are a matter that requires more attention, not just by lawmakers and oversight practitioners in the U.S. As documented by formal oversight reports, such as that from the Dutch CTIVD on automated OSINT, European intelligence services are anything but unaware that purchases of data and cross-information analysis

16 Further regional regulatory frameworks that come to mind are the second additional protocol of the Council of Europe's Cybercrime Convention and the forthcoming E-evidence regulation. They do not seem to cover voluntary modes of access, however.

tools are often underregulated and underwhelmingly overseen. This situation presents a genuine risk of disproportionate access (or worse) to commercially and publicly available data with many negative and far-reaching consequences for the protection of human rights and human dignity.

Against this backdrop, it is notable that the globally renowned EU and Council of Europe legal instruments for data protection, such as the GDPR, LED and Convention 108+, have not provided enough effective protection from these risks for at least two reasons. First, while the relevance and scope of regional legal frameworks appear to be growing for the future governance of national intelligence practice, governments will defend their exclusive right to the realm of national security by adding broad exemptions, derogations, and restrictions in such regional frameworks. Second, even if intelligence (the last true bastion of national sovereignty) had to submit to EU legislation and standards more fully on paper, their enormous enforcement deficit would still be a major concern. More specifically, the GDPR has not stopped a burgeoning market of highly sensitive surveillance data from flourishing, including within the EU.

The report therefore now turns to national legal frameworks and oversight practice for further guidance and awareness of current deficits, reform needs, and, where available, good forward-looking practices on intelligence services' non-compelled access and processing of commercially and publicly available data.

3. Deficits in national intelligence legislation and oversight practice

According to Born and Leigh, 'in a democracy, no area of state activity should be a "no-go" zone for parliament, including the security and intelligence sector' (Born and Leigh 2002: 75). Accordingly, one can expect national intelligence legislation and oversight practice to provide legitimacy for the entire spectrum of intelligence practice. The legal framework ought to provide clarity and benchmarks not just for intelligence analysts, but also for the private sector, oversight professionals, and the general public on what is permissible and what safeguards and rules have to be met.

Questions arise, however, concerning whether current national intelligence laws and oversight practice throughout Europe do so with regard to the different modes of intelligence services' non-compelled access to commercially and publicly available data as well as the status quo regarding the governance of these intelligence practices in Europe.

At the time of writing, there is hardly any comparative public knowledge about these questions, whether with regard to the rules on the books or with regard to the practice on the ground.[17] Unfortunately, providing a comprehensive review of European intelligence laws and oversight practice on this topic goes beyond the means currently available to the authors. That said, the following sections offer explorations of relevant aspects in current Danish, Dutch, French, German, and UK intelligence legislation or oversight practice. In so doing, the report identifies some important deficits and open questions that might be relevant to other European democracies as well.

3.1 Loopholes in national legislation

3.1.1. Insufficient legal basis

A key criterion for assessing the democratic governance of intelligence service access to and subsequent processing of commercially and publicly available data is whether such practices are *sufficiently* grounded in the national legal framework.

There are different views and evolving European and national jurisprudence on what, exactly, renders a legal base sufficiently comprehensive, accessible, and clear. Various constitutional and socio-legal differences between sovereign states help explain why an authoritative universal standard is unlikely to emerge. This does not mean, however, that anything goes for democracies. Indeed, there is a growing body of knowledge that lawmakers ought to consider when assessing the suitability of their current legal framework with regard to the practices discussed in the first part of this report.

By way of approximation, consider the following spectrum: At one end, a legislature may try to place each and every known intelligence activity by every single known intelligence entity on a stand-alone statutory footing. Each law would feature detailed requirements for each and every procedural step as well as detailed accounts of every technology used in the process. It would also include a thick web of safeguards and accountability requirements monitored by a multitude of different oversight bodies. Together, these bodies would ensure independent budget control, parliamentary oversight, judicial review, and data-processing audits for each and every known intelligence activity by each and every known intelligence entity. Each of these oversight bodies' investigatory powers, mandate, and resources would also

17 There are, of course, several insightful comparative reviews, for example the EU Fundamental Rights Agency's (FRA) informative comparative review of EU Member State legislation and oversight practice regarding 'general surveillance of communications' (FRA 2018: 29) and the online repository intelligence-oversight.org. Such reviews have not yet, however, extended their focus beyond direct or compelled modes of intelligence services' access to data.

be placed on a separate and equally comprehensive statutory basis. At the other end of the spectrum, imagine a country that lets its IC operate primarily on the basis of secret executive decrees and untested interpretations of the law. The actual intelligence law, by contrast, contains only general provisions which allow the IC to use (unspecified) intelligence methods to acquire, access, and process (personal) data through (unspecified) processes for the pursuit of, at best, broadly defined aims.

Both ends of the spectrum merit criticism: Excessive juridification and oversight fragmentation uses public resources unnecessarily. A legal framework is also no match for the rapid evolution of technology. Hence, some generalisation and tech-neutrality is important to avoid constant overhauls of the legal framework. That said, recent history is replete with examples of (embarrassingly) sparse general provisions in the national intelligence legislation of established democracies having to be reformed following litigation.[18]

By itself, admittedly, this provides little orientation for lawmakers. Further granularity can be added, however, by focussing on the severity of potential rights infringements through non-compelled access and subsequent data processing. More specifically, how could automated OSINT, various data purchases, and courtesy requests infringe on such rights and fundamental freedoms as the right to privacy, the right to informational self-determination, the right to free speech, and the right to free assembly?

A good starting point pertaining to every right and every practice in question is the fact that, in a democracy, every collection, retention, alteration, analysis, and transfer of personal data by the state requires a justification (Golla 2022: 10). Undoubtedly, all these practices interfere with basic rights, but the more important question concerns the threshold at which an interference becomes an infringement on or a violation of a right. Here, the BVerfG held that if interferences with fundamental rights and freedoms are not specifically authorised within a statute, then broad general clauses can only justify minor infringements to fundamental rights (ibid).[19] While this is a helpful starting point for lawmakers, it still requires complex assessments that may differ from case to case. As regards the necessary criteria to gauge whether a practice actually infringes on a basic right or fundamental freedom, one would need to consider

18 A case in point is Germany's general mandate for the foreign intelligence service in §2(1) BND Act. The German government found it to be sufficient for the practice of foreign–foreign bulk collection (similar to Executive Order 12333-type activities in the U.S.) until this became no longer tenable, both politically and legally. For more on the reform pathway from its a-legal origins via unconstitutionality towards substantial intelligence reform, see (Wetzling 2020) and (Wetzling and Vieth 2021).

19 On the distinction between minor and substantial infringements on fundamental rights, see (BGHSt. 51, 211, 218; Köhler 2021: § 161 StPO, recital 1).

- its interference with the 'core of an individual's personal life';[20]
- the degree to which the data allow agencies to pinpoint individuals;
- the number of individuals affected;
- whether or not access or collection was based on a reasonable cause;
- the accessibility of the data;
- whether or not the data remain anonymised;
- whether or not the dataset is likely to be marred by a potential bias in terms of the religious or ethnic origin of the data subjects or whether the access or collection was politically motivated;
- the secrecy of the access or collection practice;
- the amount of data accessed or collected;
- the accuracy level of the underlying software compared to the state of the art in technology and science (Rückert 2017: 320 ff; Golla 2022: 10).

It also depends, of course, on the fundamental right and specific intelligence practice in question. By way of further illustration, consider, for example, automated OSINT and the right to informational self-determination. Here, the following general conclusion from the BVerfG is insightful: 'even if the individual goes out in public, the right of informational self-determination protects his or her interest that the associated personal information is not collected in the course of automated information collection for storage with the possibility of further exploitation' (BVerfGE 120, 378 <67>, own translation).

While the BVerfG recognised the fact that systematic open-source collection and analysis might interfere with the right to self-determination, it also clarified that not every interference amounts to an infringement or violation of this right. More specifically, it held that there is

> *no encroachment on the general right of personality if a state agency collects communication contents that are available on the Internet addressing all readers or at least a group of individuals that is not further delimitated. This is the case, for instance, if the authority calls up a generally accessible Web site on the World Wide Web, subscribes to a mailing list that is open to all comers or monitors an open chatroom (BVerfGE 120, 274 <308>).*

20 In its 'sphere theory', the BVerfG distinguishes between different spheres of personal life. The innermost sphere is the core sphere. It is the *forum internum*, where feelings and thoughts are located. Hence, it includes the most intimate information about a person's life. The German basic law grants this intimate sphere absolute protection against any state interference through its human dignity clause (Art. 1 German Basic Law). For more information, see (Bumke, Voßkuhle 2019: 115 ff.)

However, it added an important qualifier:

> *an encroachment on the right to informational self-determination can, however, apply if information obtained by viewing generally accessible contents is deliberately compiled, stored and where appropriate evaluated using further data, and a special danger emerges from this for the personality of the person concerned. A basis for empowerment is required for this (BVerfGE 120, 274 < 309>).*

As argued in the first part of this report, many modes of non-compelled access to commercially and publicly available data revolve around cross-system information analysis tools. The data, thus, are very often 'systematically collected, combined and analysed'. They are also linked to or fused with other datasets from other intelligence collection methods so as to allow for far richer profiling and analysis. In turn, this results in a higher threat to individuals' personal rights. Therefore, given that the practice of automated OSINT infringes upon the right to informational self-determination, it requires a specific legal basis in German intelligence law.

Notably, though, despite its growing density, German intelligence law does not yet provide a sufficient legal basis for automated OSINT. At present, the German government can only refer to the general clause in §2 (1) BND Act[21] as the legal basis for automated OSINT by Germany's foreign intelligence service, the Bundesnachrichtendienst (BND). Similarly, automated OSINT by the federal domestic intelligence agency, Bundesamt für Verfassungsschutz (BfV), does not yet seem to have a sufficiently clear and comprehensive legal basis either. Such a basis would arguably have to be based on the general clause in §8 (1) BfV Act.

An argument whether or not these general clauses provide a sufficient legal base to justify the encroachment on the right to informational self-determination through large-scale automated OSINT is something that requires further recourse to the evolving jurisprudence of the BVerfG – including its recent landmark decision on the unconstitutionality of key provisions within the Bavarian framework for its

21 Unfortunately, there is no formal translation of German intelligence legislation. For further illustration, consider our own translation of the general clause in §2 (1) BND Act:
'(1) The Federal Intelligence Service may process the necessary information, including personal data, unless the applicable provisions of the Federal Data Protection Act or special regulations in this Act conflict with this,
1. to protect its staff, facilities, objects and sources against activities that pose a threat to security or intelligence activities,
2. for the security screening of persons who work for it or are to work for it,
3. for the verification of the intelligence access necessary for the fulfilment of its tasks, and
4. about events abroad which are of foreign and security policy significance for the Federal Republic of Germany, if they can only be obtained in this way and no other authority is competent to collect them.

Processing is also permissible if the data subject has consented.'

domestic intelligence service.[22] This may be of limited interest to international readers. Suffice to say, therefore, that the argument would need to revolve around principles and rules such as

- the doctrine of definiteness or principle of legal certainty (*Bestimmtheitsgebot*): rules must be clear and definite, especially when statutes limit basic rights: 'the indefiniteness of a statute that limits basic rights represents an additional (factual) encroachment on basic rights. Therefore, if a statute does not fulfill the attainable degree of definiteness, this must be justified by the specific need for statutory flexibility in the respective legislative field' (Papier and Möller 1997: 177);
- the doctrine of essential matters (*Wesentlichkeitstheorie*): all questions of constitutional significance ought to be regulated within the law itself (and not in executive decrees);
- the citation rule (*Zitiergebot*): if a statute is intended to permit an interference with constitutionally protected rights, Article 19 of the Basic Law requires the statute to explicitly mention the rights from which derogation is permitted;
- prohibition of excessive measures (*Übermaßverbot*): the more severely an individual freedom is restricted, the more significant the pursued interests of the common good must be (BVerfG 1 BvR 781/21);
- the principle concerning the innermost sphere of private life (*Kernbereich persönlicher Lebensgestaltung*): to protect the development of one's personality, a person can reasonably expect that an innermost sphere of private life will not be surveilled. 'This includes the possibility of expressing one's internal processes, sensations, feelings, thoughts, opinions, and experiences of a most personal character, in particular through non-public communications with trusted persons' (BVerfG 1 BvR 1619/17, 276, own translation).[23]

Despite its complexity, the relevance and result of such an assessment are, of course, anything but merely academic. Were the BVerfG to conclude in a future decision that automated OSINT infringes substantially on basic rights and fundamental freedoms (as argued by CTIVD 2022), then the need arises for a comprehensive legal basis rather than a general catch-all provision. Furthermore, and staying with

22 This decision is of key importance for federal intelligence reform in Germany given that many provisions of the federal legal intelligence framework resemble those deemed unconstitutional in Bavaria. For a discussion see (Deutscher Bundestag 2022)

23 According to the BVerfG, 'the core area of private life claims to be respected in the face of *all surveillance measures*. If they can typically lead to the collection of data relevant to the core area, the legislature must create regulations that guarantee effective protection in a clear normative manner' (BVerfG 1 BvR 1619/17, 278).

the hypothetical case of a future court decision, in the absence of a substantial legal basis, the government might eventually have to cease its automated OSINT practices. A previous decision by the BVerfG on data retention already found that the enumeration of the tasks of the BND, for example, do not suffice to justify substantial infringements of basic rights (BVerfGE 125, 260 <331 f.>).

It is thus important that lawmakers, in Germany and elsewhere, address the many open questions regarding the legal basis for non-compelled access to commercially and publicly available data through automated OSINT, data purchases using informants, or simple courtesy requests or gifts obtained from private companies.

When it comes to data purchases, lawmakers ought also to consider whether they have done enough to ensure that the IC acquires only data that were originally collected in a lawful manner. In other words, data purchases may only be allowed if the IC is legally entitled to access such data and if the data were lawfully acquired by the broker.

When it comes to courtesy requests, voluntary submissions or gifts, it is crucial to provide clarity regarding if and when such government access through 'informal means' may exceptionally be allowed. As a rule, and this ought to be stated more clearly in legislation, informal exchanges of datasets between private actors and public authorities, for example footage from Amazon Ring cameras (Guariglia and Kelley 2022; Scheuer and Neuerer 2022), are not permissible in the absence of formal authorisation and oversight procedures. Such clarity is important to ensure that such practices do not evade scrutiny and that the subsequent use of such data adheres to clear principles that are independently overseen.

3.1.2. Ambiguous terminology and insufficient safeguards for OSINT in legislation

Some European legislatures have made further inroads into this complex policy field and provide a specific legal basis for OSINT. The Dutch national intelligence law (Wiv 2017), for example, includes provisions on publicly available data and OSINT. It distinguishes between non-systematic and systematic collection of publicly available information and prescribes an authorisation process for the latter.

This said, current Dutch OSINT practice operates with an unreasonably broad conception of publicly available data. It includes 'closed websites that require registration and/or payment' (CTIVD 2017: 10, own translation) and – as reported by the Dutch intelligence oversight body CTIVD in its 2022 report on automated OSINT – data obtained on the darknet and data offered commercially by a provider (CTIVD 2022: 15-16).

This broad conceptions merits critical reflection. Should data whose origin may not be clearly established and which may only be sold to a very limited group of government clients fall under the same protection standard as data that everybody can obtain from publicly available websites? Apparently, the current Dutch legislator does not consider intelligence services' paying for services on the basis of data from unclear origins to be a threshold requiring stricter restrictions and additional safeguards. This position seems untenable going forward – at least as long as a seller's economic incentive trumps poorly enforced GDPR conformity.

3.1.3. Various human intelligence (HUMINT) loopholes

It is remarkably easy for government agencies to obtain veritable treasure troves through insufficiently regulated, let alone independently overseen, human intelligence (HUMINT)– private sector interactions. As stated by Adam Klein, former chair of the U.S. Privacy and Civil Liberties Oversight Board (PCLOB) during recent testimony: 'If I were a foreign intelligence agency and I wanted to purchase highly sensitive data, I wouldn't simply walk up to the front door, knock and announce that I'm here from the Ministry of State Security. I might, hypothetically, create a front company based in a friendly neighbouring country that looks more innocuous to facilitate the transaction'.[24]

Setting up a front company and being dishonest about its objectives in future transactions with the private sector may not just appeal to foreign adversaries, however. The following country-specific elaborations discuss how current HUMINT frameworks may give rise to creative non-compliance and disproportionate government access to commercially and publicly available data.

The UK's Covert Human Intelligence Sources Act of 2021, for example, provides an 'express legal basis for intelligence agencies, LEAs and some other public bodies to continue to use authorised undercover officers and *other* covert human intelligence sources (CHIS) to participate in crime for the greater good, such as to disrupt and detect more serious crime or safeguard national security' (Investigatory Powers Commissioner's Office 2020: 17; emphasis added). Notice the distinction between 'authorised undercover officers', for example a member of the police or intelligence agency acting under cover, and *other* CHIS.[25] The latter could be a member of the

24 Oral Testimony before the U.S. Senate's Judiciary Subcommittee on Privacy, Technology, and the Law. Available at: https://www.judiciary.senate.gov/meetings/protecting-americans-private-information-from-hostile-foreign-powers

25 According to the RIPA, a person is a CHIS, if 'he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of the following things: "covertly [using] such a relationship to obtain information or to provide access to any information to another person" or "covertly [disclosing] information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship"' „„Quoted from (Scott 2022: 1227).

public, a criminal engaging in some specific activity, or, as the case may be, an 'honest agent' working in a private-sector data-rich environment and thus uniquely positioned to pass information or databases on to the authorities.

Hypothetically, a CHIS authorisation might be issued to obtain access to datasets from the private sector that the government might not have been able or willing to formally compel through recourse to the warrant scheme of the IP Act. Alternatively, even if private sector entities could be compelled to provide access to such data through the IP Act, the process might be cumbersome and imbued with stricter accountability obligations. These limitations may serve as an incentive to improperly extend the use of CHIS authorisations.[26]

Next to the standard CHIS authorisations within the Regulation of Investigatory Powers Act (RIPA), the 2021 CHIS Act added the power to grant a 'criminal conduct authorisation' (CCA). While the Investigatory Powers Commissioner (IPC) needs to be notified of CCAs within seven days, scholars have observed that the UK legal framework places 'CCAs (far) lower on the hierarchy of intrusiveness than [...] almost any of the state's more traditional investigatory powers' (Scott 2022: 1238) and noted, in particular, 'how weak are the safeguards, both ex ante and ex post, on the use of the power, particularly when juxtaposed to those which apply to the powers introduced or reformed by the Investigatory Powers Act 2016' (ibid: 1244).

Covert HUMINT activities may indeed be necessary to protect our open societies. Yet, given their abuse potential, they need to be adequately and independently controlled. Matters such as CHIS and CCAs and their corresponding authorisation process may, despite their current complexity, need to be hardened against further risks of non-compliance and malfeasance. Recent inspections by the UK's intelligence oversight body, the IPCO, encountered 'issues' such as 'insufficient written consideration by the authorising officer (AO); lack of regular reviews for CHIS cases; a lack of timely cancellations; and the inconsistent application of the correct authorisation periods both initially and at renewal' (IPCO 2020: 47). Granted, the fact that such matters are being reported is, in and of itself, a sign of effective oversight. However, legislators, not just in the UK, ought to critically assess the relative ease with which less rigorously regulated and overseen HUMINT practice might give rise to disproportionate access to commercially and publicly available data.

Notice, for example, how the Dutch intelligence legislation stipulates that whenever 'an employee, using a false identity, or a third party under the direction and instruction

26 Alongside the standard CHIS authorisation, the 2021 reform added the power to grant a CCA.

of the service acquires a bulk dataset, the agent scheme applies' (CTIVD 2017: 10, own translation).[27] This agent scheme, however, is extraordinarily generous to the Dutch IC and in need of an update because whenever AIVD or MIVD gain access to data through informants or agents, such data are still considered open-source.[28] Given the various different ways in which undercover officers or CHIS can obtain access to enormous amounts of commercially available data, and given that OSINT data are less rigorously regulated and overseen, such a broad approach invites malfeasance and creative non-compliance.

Germany, arguably, is in a unique position to render its HUMINT legal and oversight framework fitter for the many challenges tied to government access to commercially and publicly available data. The recent landmark decision by the BVerfG on the Bavarian law on domestic intelligence (see Section 3.1.1.) found, for example, that the provisions governing the use of authorised undercover officers (*Verdeckte Mitarbeiter*) and CHIS (*Vertrauensleute*) lacked sufficiently clear rules on appropriate legal thresholds (legitimate aims) and did not sufficiently reduce the possible scope of these measures. In addition, it required far more rigorous ex ante oversight over these (and other) measures used by domestic and foreign intelligence services alike. This landmark decision, and the fact that the current government coalition has pledged to review, assess, and, if needed, reform German intelligence law, brings momentum and orientation to future discussions on the governance and oversight of HUMINT, too.[29]

Lawmakers throughout Europe would be well advised to be more attentive to a possible correlation between poorly regulated and overseen HUMINT and disproportionate government access to commercially or publicly available data. As indicated, many pathways are imaginable, such as setting up and maintaining front companies and using informants or CHIS to obtain access to large datasets in a non-compelled fashion.

3.2. Deficits in oversight practice

Assessing the democratic governance of intelligence practice, one obviously needs to consider not just what is (or, as the case may be, what is not) in the books, but also actual practice on the ground. Naturally, given the secrecy of intelligence conduct, there are limits to what researchers can objectively report in this area. Yet, one can

27 Referring to Wiv 2002, Article 21 and Wiv 2017, and Article 41.
28 Collection of data through consultation of informants (informant regulation), see Wiv 2017, Article 39.1 and Wiv 2002, Article 17.1(a).
29 For further discussion on current reform plans and needs, see Krempl (2022) and Steinke (2021).

and should extend the focus to the more open side of secrecy, namely intelligence oversight. It can give legitimacy to intelligence practice and may ensure the legality and propriety of intelligence conduct. As argued below, oversight also needs to catch up with the paradigm shift in intelligence practice that the ubiquity and easy availability of commercially and publicly available data seem to have propelled.

3.2.1. Insufficient awareness of risks

The genuine risks of government malfeasance, abuse, and disproportionate access inherent in automated OSINT and data purchases do not sufficiently appear on the radar of oversight practitioners. Consider, by way of illustration, how the Danish intelligence oversight body Tilsynet med Efterretningstjenesterne (TET) reports on Denmark's defence intelligence service's (DDIS) procurement and processing of OSINT:

> *DDIS' obtaining of information via open sources – also referred to as OSINT – includes sophisticated and systematic collection of information from, among other things, the internet, for example communication in open net forums, as well as printed media, television, etc. DDIS' compliance with OSINT legislation only requires that the information may be of significance to DDIS' intelligence related-activities directed at conditions abroad and that the information must be publicly available. [...]*
>
> *For purposes of its check thereof, in 2021 TET performed a check of one of DDIS' systems for processing information collected via OSINT and an inspection of parts of DDIS' infrastructure for handling information procured from open sources. TET's check of DDIS' procurement and processing of open source information does not give rise to any comments (TET 2022: 16, emphasis added).*

Unfortunately, OSINT inspections are not standard oversight practice in many European countries. Thus, the fact that TET subjected the DDIS' procurement and processing of OSINT to independent scrutiny and reported publicly about it shows that the Danish oversight body is prepared to exceed standard requirements.

It is surprising, however, that the report on the inspection merely states that the reviewed practice did not give rise to any commentary. This statement merits further reflection because of the genuine risk, beyond Denmark, of course, that intelligence services perform what may be called 'gestural compliance' and/or that oversight bodies stage 'accountability theatre'. More specifacally, while the individual inspection might not have given rise to comments, the TET reviewed only one of several OSINT data-processing systems and only parts of the DDIS infrastructure for handling information procured from open sources. Thus, TET could have qualified its finding

and, perhaps, even highlighted the general abuse potential tied to OSINT and the need for further regulation and a more rigorous oversight mandate. Given the various open questions regarding the scope of publicly available data (see Section 3.1.2.) and the authorisation requirements for systematic OSINT collection in some countries, and considering the fact that these data are often fused with data obtained from direct and compelled modes of access in cross-system information analyses, TET could have alerted readers to this being an evolving practice that needs more commentary, and, possibly, oversight innovation. Instead, at least on this important matter, the TET adopted an approach which appears unduly credulous to us.

Other oversight bodies, such as the Canadian National Security and Intelligence Review Agency (NSIRA) and the UK's IPCO, have recently reported on pending examinations regarding the governance and compliance of OSINT activities (NSIRA 2021: 40) so as to ensure that the 'exponential growth of online activity by LEAs, particularly in relation to open source and social media' is 'properly identified and authorised, and that material is properly handled' (IPCO 2020: 83).

3.2.2. Absence of review mandates

Some legislatures are responsible for a rather fragmented oversight landscape. In Germany, for example, different bodies perform very similar judicial review tasks, albeit with different remits and resources depending on whether the reviewed entity performs domestic, domestic–foreign, or genuinely foreign surveillance (G-10 Commission and the Independent Control Council, respectively). It may not be easy, in such a context, to entrust a particular oversight body with reviewing the IC's access to and subsequent processing of commercially and publicly available data. At the moment, unfortunately, German intelligence legislation does not specifically mandate a particular intelligence oversight body to perform ex ante and ex post oversight for the non-compelled modes of access described in Part I of this report.

3.2.3. Insufficient review mandates

Governments may sometimes be inclined to paint a rosy picture of national oversight practice. For example, they may have this inclination when interacting with the judiciary in litigation proceedings or when elaborating on national standards vis-à-vis standards in other countries in international negotiations aimed at securing data free flow with trust (DFFT).

A classic tale often told in such situations is the ability of oversight bodies to perform unannounced inspections anywhere on the premises of the intelligence services during which, apparently, every aspect of intelligence conduct is subjected to rigorous scrutiny. By contrast, de facto oversight may not be so comprehensive.

In part, this may be due to human-related factors, for example when oversight practitioners entertain too cosy relationships with intelligence professionals, which, in turn, may affect the impartiality of their assessments. Some practitioners may also lack the motivation to pursue proactive and unglamorous oversight. At times, inspections may require what intelligence veteran Herbert E. Meyer refers to as a 'helicopter-raids at dawn, breaking down-the-doors, kick-rear-ends' (Meyer 2003) determination to find answers. Moreover, underwhelming oversight performance may also result from scarce resources and limited technical expertise. Equally importantly, oversight bodies may lack the comprehensive access to the IC's IT systems and operational databases which is needed to perform data-driven intelligence oversight in this day and age (Vieth and Wetzling 2019). All these factors might significantly reduce the actual impact of overseers' access to the premises of the IC.

Furthermore, oversight bodies tend to focus on the precise catalogue of oversight tasks attributed to them in national legislation. Consequently, if the formal oversight mandate does not (yet) include rigorous reviews of and reporting on data purchases and the subsequent processing of commercially and publicly available data, then it is very unlikely that many oversight bodies will go beyond their formal mandate and launch a sui generis inquiry into the matter, let alone perform audits and review contracts for data purchases. France is a case in point here. The systematic and automated collection of OSINT is not part of the formal Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) review mandate (Tréguer 2022); nor is the matter reported in its annual report (CNCTR 2022).

In response to this deficiency, one must remind European lawmakers to not only add provisions and safeguards regarding intelligence services' access to and processing of commercially and publicly available data into the legal framework, but to also seize the opportunity to broaden the formal mandate of oversight bodies accordingly.

As argued above, this need to extend oversight remits also pertains to the necessary reforms regarding the governance of HUMINT. For example, as German lawmakers are writing more elaborate safeguards regarding the use of authorised undercover officers and CHIS into the federal intelligence framework following the recent decision by the BVerfG, they ought to remember that this, too, requires independent ex ante authorisations, not just once per mission but at several intervals if the duration of the mission so requires (BVerfG, Judgement of the First Senate from 26 April 2022, – BvR 1619/17 –, recital 348).

Furthermore, given the potential for different modes of access and processing of commercially and publicly available data to encroach on the 'innermost sphere of private life' (*Kernbereich privater Lebensgestaltung*), an 'independent review of the results of the surveillance' and, by consequence, modifications to the existing oversight remit are also required (BVerfG, Judgment of the First Senate from 26 April 2022, – 1 BvR 1619/17 –, recital 282, own translation).

3.2.4. Failure to reflect the combined effect of different surveillance measures

The combined effect of different surveillance measures on an individual's enjoyment of fundamental rights and freedoms is another aspect which may not be sufficiently reflected in actual oversight practice. Many such combined effects are imaginable, such as when several ongoing surveillance measures may simultaneously interfere with an individual's rights or when intercepted personal data are subsequently enriched or pooled (for richer profiling and analysis) with data from purchased datasets or gathered from the darkweb. Such data enrichment or cross-system interlinkages merit more attention from oversight bodies.

Greater attention is required, in particular, because 'the proportionality of a single surveillance measure depends also on the existence and scope of further surveillance measures' (BVerfG, Judgment of the First Senate from 26. April 2022, – 1 BvR 1619/17 –, recital 290, own translation). Accordingly, the BVerfG held that 'effective oversight generally requires that the review body can scrutinise all surveillance measures that an individual may be exposed to' (ibid). By contrast, and this point is tied to the need for comprehensive access to the IC's IT systems and databases discussed above, the Court found that 'the extent and the legality of a surveillance practice and the potentially inherent infringement of cumulative rights may not be reliably assessed if the review body only has access to a limited set of data' (ibid).

As regards oversight body access to data, one needs to also take into account that some intelligence practices do not even require the acquisition of the data, for example when third parties hold the data for them in a cloud space, begging the question of whether the oversight bodies also have access to such cloud space.

Considering and assessing the combined effect of different surveillance measures is a matter that relates to both ex ante authorisation and ex post review of data processing. Warrant applications, for example, could include such consideration and assessment as criteria both for the applicant to address and for the authorising institution to verify. Likewise, independent inspections to assess the legality of data processing may test against this criterion.

4. Summary

The previous discussion has shown how selected European legal frameworks for intelligence practice are not yet fit for purpose when it comes to securing rights-based and proportionate acquisition as well as lawful processing of commercially and publicly available data by the IC. In addition, oversight practice is beset by a wide range of deficits in this regard. Presumably, this finding transcends the national contexts selected.

Part III: Pointers for progress

As argued in Part II of this report, current legal frameworks and oversight practice in key European democracies are not fit for the purpose of securing lawful and proportionate government acquisition and processing of commercially and publicly available data. This situation poses tremendous risks to the protection of human rights and the rule of law and needs to be rectified.

Yet, what kind of regulations and safeguards should democracies put in place to remedy current deficiencies? How can intelligence oversight bodies meaningfully contribute to the governance and review of intelligence practices that have not yet received much public attention in Europe? What competencies and resources do oversight bodies need in this regard, and what review and investigatory powers must they have?

The final section of this report discusses ideas and recommendations that, it is hoped, will give lawmakers, oversight bodies, researchers, and the interested general public pointers for progress. The recommendations are neither exhaustive nor definitive, however. Clearly, there can be no blueprint for how democracies might remedy their common deficits in this policy field due to the many constitutional and socio-political differences that exist across them. That said, a comparative review can often be a source of inspiration.

The following ideas reflect the authors' ongoing dialogue with oversight practitioners within the European Intelligence Oversight Network (EION). We invite readers and intelligence governance practitioners to share any comments on or reactions to the points mentioned below.

1. Recommendations, ideas, and food for thought

1.1. Further international engagement is necessary

European lawmakers ought to do much more to ensure that data brokers do not gain access to certain types of data in the first place. What is more, the limited interactions data brokers may still have with security agencies ought to be rule-based and independently overseen. A good milestone for this would be to refine and then to adopt a '**whole of privacy approach**' as regards the future regulation and oversight practice of these currently non-compelled modes of intelligence

collection. If such data are collected and processed for commercial purposes, they are still likely to be obtained by the IC, which will use them for secondary purposes. In order to make the private sector's initial collection of data and its subsequent data aggregation for security agencies more rule-based and restricted, the GDPR must be applied and enforced more strictly. Doing so requires further refinements to European data protection frameworks and a closer alignment and synchronisation with accountability mechanisms that are geared towards the public sector. More specifically, lawmakers and decision-makers should

- improve the de facto effectiveness of the GDPR. This, obviously, is an enormous and pressing endeavour. Among the many steps necessary would be extending the remit of the EDPB to a wider range of cross-border cases;
- call on their national governments and fellow lawmakers to ratify their countries' membership of Convention 108+ of the Council of Europe, the only international legal framework that does not waive safeguards when data processing takes place for security and defence purposes.

1.2. Render current legal frameworks more 'foreseeable'

According to the jurisprudence of the European Court of Human Rights (ECtHR), the quality of a law is determined not just by its accessibility to the people but also by its *foreseeability*. With the latter, the ECtHR held that national legislation 'must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to [...] potentially dangerous interference with the right to respect for private life and correspondence' (ECtHR, Malone v. the United Kingdom, application no. 8691/79, § 67).[30] It is precisely with regard to the forseeability of intelligence laws that most European democracies have substantial room for improvement. More specifically, lawmakers ought to do more to adopt a **comprehensive and sufficiently foreseeable legal basis** when it comes to the practices discussed in Part I.

First, as regards **automated OSINT**,

- more **safeguards** are necessary with regard to the purchase and use of OSINT analysis tools, including requirements relating to the different data types that can be used to feed cross-system information analysis tools;

30 On the ECtHR's increasing scrutiny of 'whether Member States' legislative branch had respected the principles of the rule of law and the minimum requirements of good law-making', see (van der Sloot 2022).

- reformers should **trim the working definition for publicly available information** and establish clearer boundaries between systematic and non-systematic collection;[31]

Promising idea: *A forthcoming amendment of the Dutch Code of Criminal Procedure regards open-source collection as 'systematic' when it is 'reasonably foreseeable that a more or less complete picture of certain aspects of the personal life of the data subject can be obtained' (CTIVD 2022). Among the factors to be taken into account are the size and type of data, the nature of the data, the way in which queries are effectuated, how data are saved and used, and the possible consequences for a data subject;*

- reformers should specifically address the **risk of so-called additive rights' infringements that arises when the proportionality of a single surveillance measure can no longer be assessed without simultaneously taking into account also how this particular measure interacts with other ongoing surveillance measures and their combined analysis.** Many cross-system information analysis systems fuse broadly defined publicly available information with bulk data emanating from other modes of intelligence collection, such as SIGINT and CNE. This practice thus constitutes additional rights' interferences, and in order for it to be justified and proportionate, additional safeguards and oversight practice ought to be introduced. As stated by the BVerfG, 'it is possible that various individual encroachments, in themselves insignificant, on areas protected by fundamental rights, in their total effect result in a serious impairment which exceeds the degree of intensity of encroachment that can be constitutionally accepted' (BVerfGE 123, 186 <266>);

Food for thought: *Many commercially available datasets comprise aggregated open-source data, but intelligence agencies also perform OSINT themselves. Following this logic, every type of data not protected by specific safeguards could be considered to be openly available by the services. This scenario, too, requires far more critical legislative attention when it comes to future rules on the intelligence services' recourse to 'publicly available information'.*

Second, as regards **the purchase and subsequent processing of commercially available data**,

31 Notice that the LED and the GDPR offer no further guidance in this regard. Accordingly, safeguards for sensitive data depend on whether such data have been 'manifestly made public' (LED Art 10, GDPR, Art 9). However, the scope of such manifestations remains disputed.

- **provisions in national intelligence law should be adopted on government access to personal data through data purchases**, including better **safeguards** to ensure the legality of data purchases, data analysis tools, and the subsequent use of data from non-compelled access;
- any such reform should try to seek an **appropriate balance** between the interests at stake in processing the data for the relevant intelligence investigation and the severity of the breach of the fundamental rights of the data subject. For example, processing data from a leaked dataset constitutes a larger interference with the fundamental rights of a data subject than processing data from (news) sources that are accessible to everyone. This ought to be reflected more explicitly in the governance processes that lead to a decision on whether or not to acquire a commercially available dataset.

Third, as regards the reception of **voluntary submissions of personal data** by the private sector, courtesy requests, and gifts,

- lawmakers should establish clarity for when such access may be permissible and what processes should be followed so as to promote proportionate processing and effective oversight. Such oversight could be achieved through the introduction of documentation and tagging requirements, as well as data minimisation, retention, and deletion obligations. As a general rule, it is suggested that such government access through 'informal means' may only be allowed in exceptional cases;

Food for thought: *As a general rule, the law should explicitly state that the intelligence service can only purchase data that were legally collected/assembled by the provider/seller. These data would then also be subsumed under the national authorisation/warrant scheme. Such a scheme should include, as currently practised in the UK, so-called data examination warrants, that is, authorisation not just for the acquisition of data but also separate warrants for their examination.*

Fourth, as regards **oversight competences written into the legal framework**,

- future legal reforms should **extend the competence catalogue** for oversight bodies in the relevant statutes. For example, statutes should explicitly mandate oversight bodies to review the tools, data types, and data processes of the IC's automated OSINT;

Food for thought: *The Norwegian intelligence oversight body Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-Committee) can extend its review focus to private sector organisations that work for or with the security and intelligence sector. If the EOS-Committee learns that a service uses information provided by a private actor, it can compel access to the information it needs for its investigation directly from the private actor entity.*

Fifth, as regards potential changes to the **general (consolidated) intelligence framework**,

- democracies should ensure that their general legal framework regarding the authorisation and, more importantly, the processing of bulk data in the context of intelligence services applies to any data, irrespective of their origin. Ideally, this framework would also follow a functional logic, in the sense that any public body with investigatory powers resembling those of intelligence services, for example military intelligence, fusion centres, border guard services, and other agencies in the broader security sector, would come under this regulatory framework;

Good practice: *Intelligence laws can help to ensure that services do not retain data indefinitely by requiring, for example, that* **data need to be attached to a specific case after a limited period of access.** *This is the case, for example, in Norway, where the time limit is four months.*

- lawmakers should ensure that the IC's conduct regarding data that are not directly in its possession, such as data hosted by private cloud providers, is lawful and proportionate. Several legal frameworks apply governance standards only to acquired data, for example data that are in the possession of the services. However, **standards and oversight for data that the services may 'access but not acquire'** are increasingly important;

Good practice: *Dutch lawmakers have written more* **direct personal duty of care responsibilities** *into the law for the heads of the IC. Observers say that this step has improved the quality of the dialogue between oversight bodies and the services as the IC leadership has a more direct personal interest in effective oversight.*

Food for thought: *Services should no longer be able to implement new practices and technologies without justifying in advance why such a new practice/technology is compliant with the law. Therefore, lawmakers should*

entertain the reverse-justification notion: what if national intelligence **law obliged the IC leadership to explain and defend the legality of a novel practice vis-à-vis the oversight bodies before it can be implemented** *by the service? If this were done, oversight bodies would not only react to what the services do and what they may have found in ex post inspections. Given that the current procedure for stopping an illegal practice can be very time-consuming, and given that during oversight investigations most services are given ample time to generate written statements during which right infringements may continue, a practice whereby the services need to justify legality in advance might significantly help to increase oversight effectiveness.*

Food for thought: *Lawmakers should also discuss whether conventional distinctions between different types of data (e.g., targeted vs non-targeted and personal vs non-personal) remain useful or need to be adjusted in a field that is very dynamic and subject to various changes.*

1.3. Make oversight practice more effective

Laws can only go so far to secure rights-based and proportionate government conduct. Oversight practice is also key and in constant need of adjustment. The following segment lists recommendations for how it could be rendered more effective in the face of the growing challenge of non-compelled and insufficiently controlled access and processing of commercially and publicly available data.

- **Exploit ex ante consultations on databases and use them for oversight cooperation**

Good practice: *The German legal framework requires so-called file orders (database establishing orders) for each automated database that the services wish to operationalise. Such orders ought to contain very specific information: the name of the database, its purpose, the requirements regarding retention, transfer, and use (including information on the group of persons to be affected and the type of data used), origins of the data, access restrictions, dates for required reviews, and protocol requirements (§ 14 BfV Act). By law, this information is to be made available not just to the government for its executive controls, but also to the federal DPA. It needs to be consulted prior to the operationalisation of each new database,*[32] *no matter the origin of the data therein.*

32 Exceptions to this requirement for ex ante consultation are permissible in urgent cases; see §14 (3) BfV Act.

> *The DPA can put this information to good use as the totality of file orders (database establishing orders) can give independent supervision bodies substantial knowledge on the variety of different IC databases and the data types therein.*[33] *Its positive effect can further be strengthened through oversight cooperation. For example, sharing that knowledge with review bodies might influence future authorisation decisions;*[34]

- **Introduce mandatory inventories of all databases** and **binding powers to delete irrelevant databases.** Several oversight bodies in Europe already have the competence to control the datasets used by the services and to establish whether or not they are still in use. This general competence should be turned into a mandatory obligation to annually review the inventory of all databases;
- Oversight bodies should receive further training to verify the accuracy of data obtained through non-compelled modes of access, especially if these data are to be pooled with other sensitive data and then shared with other agencies.

> **Good practice:** *The Dutch intelligence oversight body CTIVD has the binding power to order the deletion of datasets that are no longer relevant;*

- **Enable comprehensive oversight body access to procurement contracts.**

As many researchers interested in data purchases by national intelligence agencies can testify, it is very difficult to establish through freedom of information requests the precise nature of 'bought intelligence' and contractual obligations relating to its use. One essential piece of information are the contracts between private sector entities and the government. Oversight bodies should be granted unfettered access to any procurement contract that the agencies under their remit have concluded with private sector entities.

> **Good practice:** *NSIRA has a statutory power that ensures this kind of access. According to the NSIRA Act Art. 9 (1), 'despite any other Act of Parliament and subject to section 12, the Review Agency is entitled, in relation to its reviews, to have access in a timely manner* **to any information that is in the possession or under the control of any department'**. *Importantly, NSIRA, and not other government departments, can decide whether or not the sought*

33 Such database establishing orders are only required for 'automated' databases. This would not include stand-alone datasets that informants or private sector entities may voluntarily provide to the services – at least as long as they are not linked to or synchronised with existing automated datasets. Thus, this provision, mirrored in several German intelligence laws, might need to be hardened against creative non-compliance.

34 In this regard, the German BFDI and the G10 Commission of the Bundestag will probably have to intensify their structural exchanges to more than one 'jour fixe' per year (BFDI 2022: 75). It is hoped that the importance of genuine oversight cooperation will be reflected in more action going forward.

> *information relates to a review or complaint. NSIRA is also entitled to have access to any protected information, such as information 'under the law of evidence, solicitor–client privilege or the professional secrecy of advocates and notaries or to litigation privilege'.*

- **Verify adherence to the 'need to know' principle** more rigorously. Another aspect that the legal framework and oversight practice should look into is whether the 'need to know' principle is sufficiently applied. Put differently, sensitive data do not need to be available to each agency and each and every agent. For example, access to leaked data can be restricted to persons with certain functions, or such persons can be required to acquire additional authorisation to access data. In this regard, a 2017 CTIVD report includes helpful information regarding the 'application of the outside-in procedure with its separation of functions and tasks aimed at the need-to-know principle and the use of a retention period (in excess of the law)' as 'application of careful data processing' (CTIVD 2017: 21) when it comes to datasets containing personal data.

1.4. Promote interdisciplinary research on supervisory technology

Intelligence and national security practice tends to be viewed as exceptional. Whenever the focus of international negotiators alights on national security practice, it often shifts from commonality to exemptions, derogations, and restrictions. At the national level, too, the lengthy process of 'intelligence democratisation' has its unique pace and objectives. There are, evidently, many good reasons why intelligence practice requires secrecy and cannot easily be subjected to the standards of good governance that might apply to other policy fields. This said, intelligence is often not unique, in the sense that very similar data-driven analysis solutions are applied in other fields and that intelligence oversight bodies could, in their turn, learn from auditing tools used in the financial markets, for example. In view of the fact that intelligence is so data-driven and oversight bodies receive more comprehensive access to the IC's IT systems and databases, it is particularly important that more research and dialogues are conducted outside the corridors of power on data-driven intelligence oversight (Vieth and Wetzling 2019). Oversight bodies should, for example, be placed in a much better position to follow what the IC is doing in real time and not only observe, in retrospective, what it did in the past.

1.5. Raise awareness and provide more public education

Lawmakers need to understand the complex practices of intelligence and, more importantly, the many risks to fundamental rights and freedoms they pose. They also need to grasp whether or not these practices are properly governed or whether law, policy, and oversight practice needs to adapt. Simply put, if parliamentarians do not understand what the services do and the risks involved, it is unlikely that a robust legal framework will emerge. In other words, it is highly unlikely that the law, and, by extension, oversight practice, will be of good quality unless the knowledge base of lawmakers is raised, too. Therein lies a call to action not only for oversight bodies but also for civil society organisations. The oversight bodies, arguably, benefit from civil society's regular outreach to politicians on how loopholes in current intelligence legislation are a risk to our open societies and how legal bases and oversight practice may be fixed or overcome. Likewise, such outreach to parliamentarians may render transparency reporting by oversight bodies more effective as the recipients of their reports may be more persuaded about the genuine importance of constant debates and, if needed, reforms.

Good practice: *Swiss and Danish oversight bodies are currently trying new ways to render oversight bodies more visible and approachable. Such bodies are increasingly seeking to publish in new ways, such as explanatory videos and posts on social media, to try to convey the essence of their work and findings in digestible formats and language. They also engage in public consultations and go to greater lengths to publish their risk-based approach to setting oversight priorities, for example.*

2. Checklist for lawmakers

Some of the recommendations listed in the previous section are more general in nature and do not only pertain to the challenge of securing rule-based and proportionate intelligence service access and the subsequent processing of commercially and publicly available data. The following checklist, by contrast, is meant to help lawmakers tackle this complex terrain of currently non-compelled modes of intelligence collection. The checklist features key ingredients that a national legislative framework and oversight practice should include for the different modes of non-compelled access listed in the table below.

Checklist for lawmakers

Types of non-compelled access to commercially or publicly available data	Sufficient legal basis?	Acquisition vs indirect access?	Ex ante authorisation	Ex post oversight	Transparency	Judicial or non-judicial redress available?
Automated OSINT	☐ sufficient ☐ insufficient ☐ absent	☐ applicable ☐ n/a	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent
Data purchases • Ad hoc • Subscription based	☐ sufficient ☐ insufficient ☐ absent	☐ applicable ☐ n/a	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent
Purchase of finished analyses	☐ sufficient ☐ insufficient ☐ absent	☐ applicable ☐ n/a	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent
HUMINT (CHIS) - data broker interaction	☐ sufficient ☐ insufficient ☐ absent	☐ applicable ☐ n/a	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent
Courtesy requests	☐ sufficient ☐ insufficient ☐ absent	☐ applicable ☐ n/a	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent
Voluntary submissions	☐ sufficient ☐ insufficient ☐ absent	☐ applicable ☐ n/a	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent	☐ sufficient ☐ insufficient ☐ absent
Relevant dimensions/questions here are:	→ Is the legal framwork sufficiently clear and forseeable and does not solely rely on general provisions? → Has it been adopted by parliament with the possibility of pre-legislative scrutiny for civil society?	→ Is a data establishing order possible/necessary? → Do standard data processing obligations apply to this kind of data?	→ Is a warrant scheme necessary/applicable? → If so, can the main criteria from existing warrant schemes for other intelligence collection modes be applied here?	→ Do review bodies have sufficient access to data and tools used for the analysis of purchased data or OSINT?	→ Public reporting on data purchases and OSINT as well as the subsequent use of cross-in-formation-analysis tools? → By whom? → How often?	→ For whom? → Which entity should be responsible for complaints? → Does this entity fulfil the criteria for effective remedies spelled out in recent European Court decisions?

Conclusion

Current EU privacy and data protection regulations as well as the national legal frameworks for intelligence collection and intelligence oversight practice in key European democracies are not yet fit for purpose to secure lawful and proportionate government acquisition and processing of commercially and publicly available data. This, in essence, is a key finding from Part I and Part II of this report.

The paradigm shift in intelligence collection that these practices embody requires further research and much more legislative attention, and not just in the U.S. In fact, given the wide range of open questions and deficits identified throughout this report, we argue that governments' non-compelled access to commercially and publicly available data should now become the next frontier of intelligence law and policy reform.

Due to the rapid evolution of technology and the growing density of public–private co-productions of intelligence, it is important to actively engage different stakeholders in the quest for good answers to these important governance questions. Our democracies need pioneers with sufficient ambition, expertise, and power to collectively rein in 'unsavvy' data purchases and unduly broad OSINT practices. We hope that this report helps draw the attention of the many stakeholders interested in good intelligence governance to this complex matter. They may be inspired by the initiatives, ideas, and transferable good governance practices highlighted in Part III of this report. They may also remember that 'few nations have spotless hands in the murky world of intelligence' (Klein 2022: 7). Consequently, reformers should approach the quest for better governance with humility and avoid undue politicisation. Reformers will also need to be mindful of the genuine and imminent security threats that our open societies currently face. These threats must be met resourcefully, and data-driven intelligence, as currently shown in Ukraine, is a vital component of doing so – but so are appropriate legal frameworks and democratic safeguards as well as effective and data-driven oversight. All these practices prevent undue duplication and accountability shirking and establish much-needed legitimacy for intelligence practice.

Ideally, the quest for better governance of currently non-compelled and poorly overseen modes of intelligence collection will thus be evidence-based and undogmatic. The common aim of reformers should be to insulate democracies from illiberal practice whilst not abandoning key instruments for their security.

Glossary

AIVD	Algemene Inlichtingen- en Veiligheidsdienst (Dutch Intelligence Service)
AO	Authorising Officer
BfV	Bundesamt für Verfassungsschutz (German Federal Domestic Intelligence Service)
BND	Bundesnachrichtendienst (German Federal Foreign Intelligence Service)
BVerfG	Bundesverfassungsgericht (German Federal Constitutional Court)
BVerfGE	Bundesverfassungsgerichtentscheidung (Decisions of the German Federal Constitutional Court)
CCA	Criminal Conduct Authorisation (UK)
CHIS	Covert Human Intelligence Sources (UK)
CJEU	European Court of Justice
CNCTR	Commission Nationale de Contrôle des Techniques de Renseignement (French intelligence oversight body)
CNE	Computer Network Exploitation (Hacking)
CTIVD	Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten (Dutch intelligence oversight body)
DDIS	Forsvarets Efterretningstjeneste - FE (Danish Defence Intelligence Service)
DFFT	Data Free Flow With Trust
DPA	Data Protection Authorities

DSA	Digital Services Act (EU)
EDPB	European Data Protection Board
FRA	Fundamental Rights Agency (EU)
EOS-Committee	Stortingets Kontrollutvalg for Etterretnings-, Overvåknings- og Sikkerhetstjeneste (Norwegian intelligence oversight body)
ECtHR	European Court of Human Rights
GDPR	General Data Protection Regulation (EU)
HUMINT	Human intelligence
IC	Intelligence community
IPC	Investigatory Powers Commissioner (UK)
IPCO	Investigatory Powers Commissioner's Office (UK)
LEA	Law enforcement agency
LED	European law enforcement directive (EU)
MIVD	Militaire Inlichtingen- en Veiligheidsdienst (Dutch intelligence service)
NATO StratCom COE	NATO Strategic Communications Centre of Excellence
NSIRA	National Security and Intelligence Review Agency (Canada)
NTTC	National Travel Targeting Center (Belgium)
OSINT	Open-source intelligence
PCLOB	Privacy and Civil Liberties Oversight Board (USA)
RIPA	Regulation of Investigatory Powers Act (UK)

SIGINT	Signals intelligence
TET	Tilsynet med Efterretningstjenesterne (Danish intelligence oversight body)
TEU	Treaty Establishing the European Union

Bibliography

Biddle, Sam. 2022. *Amazon admits giving ring camera footage to police without a warrant or consent.* Available at: https://theintercept.com/2022/07/13/amazon-ring-camera-footage-police-ed-markey/

Boehme-Neßler, Volker. 2016. *Das Ende der Anonymität: Wie Big Data das Datenschutzrecht verändert.* In: Datenschutz und Datensicherheit 40. 419-423.

Born, Hans and Ian Leigh. 2005. *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence.* Available at: https://www.dcaf.ch/sites/default/files/publications/documents/making-intelligence.pdf

Bradford Franklin, Sharon, Greg Nojeim and Dhanaraj Thakur. 2021. *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers.* Center for Democracy and Technology. Available at: https://cdt.org/insights/report-legal-loopholes- and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/

Brayne, Sarah. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing.*

Bumke, Christian and Andreas Voßkuhle. 2019. *German Constitutional Law: Introduction, Cases, and Principles*. Oxford, New York: Oxford University Press. Available at: https://global.oup.com/academic/product/german-constitutional-law-9780198808091?cc=de&lang=en&

Burke, Garance and Jason Dearen. 2022. *Tech tool offers police 'mass surveillance on a budget'*. Available at: https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef

Cameron Iain. 2021. *Metadata retention and national security: Privacy International and La Quadrature du Net*. Common Market Law Review, Vol. 58, No. 5: 1433-1472. Available at: https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/58.5/COLA2021088

Council of Europe. 2022. *Chart of signatures and ratifications of Treaty 223*. Available at: https://www. coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 (Status as of 2 June 2022)

Cox, Joseph. 2022. *Revealed: U.S. Military bought mass monitoring tool that includes internet browsing, email data.* Available at: https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data

Cyphers, Bennett. 2022. *Inside Fog Data Science, the secret company selling mass surveillance to local police.* Available at: https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police

Deutscher Bundestag, Wissenschaftliche Dienste. 2022. *Auswirkungen des Urteils des Bundesverfassungsgerichts vom 26. April 2022 zum Bayerischen Verfassungsschutzgesetz: Allgemeine Vorgaben und deren Anwendung auf das Bundesrecht.* Ausarbeitung WD 3 - 3000 – 069/22. Available at: https://www.bundestag.de/resource/blob/903554/08bb7802b3c4d487a5bdbf79bafabe64/WD-3-069-22-pdf-data.pdf

Drechsler, Laura. 2020. *The Achilles Heel of EU Data Protection in a Law Enforcement Context: International Data Transfers under Appropriate Safeguards in the Law Enforcement Directive.* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3664125

European Commission. 2022. *April infringements package: key decisions.* Available at: https://ec. europa.eu/commission/presscorner/detail/EN/INF_22_1769

European Union Agency for Fundamental Rights. 2017. *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*. Volume II: field perspectives and legal update. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf

Ferguson, Andrew G. 2017. *Policing Predictive Policing.* Washington University Law Review, Vol. 94, No. 5. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765525

Forbrukerrådet. 2020. *Out of Control: How Consumers are Exploited by the Online Advertising Industry.* Available at: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of- control-final-version.pdf

Golla, Sebastian. 2022. *Grundrechtliche Eingriffe durch Internetauswertungen*. In: Jonas Grutzpalk and Stefan Jarolimek. Polizei.Wissen: Open Source Intelligence für die Polizei.Verlag für Polizeiwissenschaft.

Guariglia, Matthew and Jason Kelley. 2022. *Ring Reveals They Give Videos to Police Without User Consent or a Warrant*. Electronic Frontier Foundation. 15. Juli 2022. Available at: https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant.

Higgins, Eliot. 2022. *We Are Bellingcat*. Bloomsbury UK. Available at: https://www.genialokal.de/Produkt/Eliot-Higgins/We-Are-Bellingcat_lid_45353477.html

Hornung, Gerrit and Bernd Wagner. 2019. *Der schleichende Personenbezug: Die Zwickmühle der Re-Identifizierbarkeit in Zeiten von Big Data und Ubiquitous Computing*. In: Computer und Recht, Vol. 35, No. 9: 565-574. Available at: s://doi.org/10.9785/cr-2019-350910

Klein, Adam. 2022. Prepared Statement before the U.S. Senate Judiciary Subcommittee on Privacy, Technology, and the Law. *"Protecting Americans' Private Information from hostile foreign powers"*, Available at: https://www.judiciary.senate.gov/download/testimony-klein-2022-09-14

Köhler, Meyer-Goßner/Schmitt. 2021. *Kommentar zur StPO*, 64. Auflage. § 161 recital 1.

Krempl, Stefan. 2022. *Karlsruher Urteil: Regierung will Verfassungsschutz-Befugnisse einschränken.* Heise online. Available at: https://www.heise.de/news/Karlsruher-Urteil-Regierung-will-Verfassungsschutz-Befugnisse-einschraenken-7146236.html

Massé, Estelle. 2022. *Four years under the EU GDPR: How to fix its enforcement.* Access Now. Available at: https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf

Meyer, Herbert E. 2003. *A memo to the 9/11 Commissio*". Available at: https://www.nationalreview.com/2003/01/memo-911-commission-herbert-e-meyer/

Mitsilegas, Valsamis, Elspeth Guild, Elif Kuskonmaz and Niovi Vavoula. 2022. *Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks*. European Law Journal. 1–36. Available at: https://doi.org/10.1111/eulj.12417

Nazareth, Craig. 2022. *Technology is revolutionizing how intelligence is gathered and analyzed – and opening a window onto Russian military activity around Ukraine*. The Conversation. Available at: https://theconversation.com/technology-is-revolutionizing-how-intelligence-is-gathered-and-analyzed-and-opening-a-window-onto-russian-military-activity-around-ukraine-176446

Ng, Alfred. 2022. *Privacy bill triggers lobbying surge by data brokers*. Available at: https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958

Papier, Hans-Jürgen and Johannes Möller. 1997. *Das Bestimmtheitsgebot und seine Durchsetzung.* Archiv des öffentlichen Rechts, Vol. 122, No. 2: 177–211. Available at: http://www.jstor.org/stable/44316314

Reviglio, Urbano. 2022. *The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview.* Internet Policy Review 11 (3). DOI: 10.14763/2022.3.1670. https://policyreview.info/articles/analysis/untamed-and-discreet-role-data-brokers-surveillance-capitalism-transnational-and

Rieke, Aaron, Harlan Yu, David Robinson, and Joris von Hoboken. 2016. *Data Brokers in an Open Society.* Upturn & Open Society Foundations. Available at: https://www.opensocietyfoundations .org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf

Rückert, Christian and Thomas Goger. 2022. *Strafprozessuale Zulässigkeit (automatisierter) OSINT-Ermittlungen – am Beispiel des Dark Web Monitors*. In: Jonas Grutzpalk and Stefan Jarolimek. Polizei.Wissen: Open Source Intelligence für die Polizei. Verlag für Polizeiwissenschaft.

Rückert, Christian. 2017. *Zwischen Online-Streife und Online-(Raster-)Fahndung – Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren*. Zeitschrift für die gesamte Strafrechtswissenschaft Vol. 129, No. 2: 302-333. Available at: https://doi.org/10.1515/zstw-2017-0012

Sajfert, Juraj and Teresa Quintel. 2017. *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*. Available at: https://ssrn.com/abstract=3285873.

Scheuer, Stephan and Dietmar Neuerer. 2022. *Überwachung: Amazons Türklingel ‚Ring' gibt Daten ohne Gerichtsbeschluss an deutsche Polizei*. Handelsblatt. Available at: https://www.handelsblatt.com/technik/it-internet/ueberwachung-amazons-tuerklingel-ring-gibt-daten-ohne-gerichtsbeschluss-an-deutsche-polizei/28669862.html.

Scott, Paul F. 2022. *Authorising Crime: The Covert Human Intelligence Sources (Criminal Conduct) Act 2021*. The Modern Law Review 85 (5): 1218–44. https://doi.org/10.1111/1468-2230.12751.

Steinke, Ronen. 2021. *Mehr Macht für Richter.* Süddeutsche Zeitung. Berlin. Available at: https://www.sueddeutsche.de/politik/geheimdienste-mehr-macht-fuer-richter-1.5187662

Transparency Market Research. 2022. *Data Brokers Market.* Available at: https://www.transparencymarketresearch.com/data-brokers-market.html

Tréguer, Félix. 2022. *Major oversight gaps in the French intelligence legal framework.* Available at: https://aboutintel.eu/major-oversight-gaps-in-the-french-intelligence-legal-framework/

Twetman, Henrik, and Gundars Bergmanis-Korats. 2021. *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data.* Nato Strategic Communications Center of Excellence. Available at: https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security _20-01-2020.pdf

van der Sloot, Bart. 2020. *The Quality of Law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases*. JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law Vol. 11, No. 2, 2020. Available at: https://www.jipitec.eu/issues/jipitec-11-2-2020/5098/

Vieth, Kilian and Thorsten Wetzling. 2019. *Data-driven Intelligence Oversight. Recommendations for a System Update*. Stiftung Neue Verantwortung. Available at: https://www.stiftung-nv.de/sites/default/files/data_driven_oversight.pdf

Wetzling, Thorsten and Charlotte Dietrich. 2021. *Report on the need for a Guidance note on Article 11 of the modernised Convention 108.* Stiftung Neue Verantwortung. Available at: https://rm.coe.int/ t-pd-2021-6-draft-guidance-note-on-exceptions-under-article-11-of-the-/1680a2d512

Wetzling, Thorsten, Lauren Sarkesian and Charlotte Dietrich. 2021. *Solving the Transatlantic Data Dilemma: Surveillance Reforms to Break the International Gridlock.* Stiftung Neue Verantwortung & Open Technology Institute. Available at: https://www.stiftung-nv.de/sites/default/files/ snv_solving_the_transatlantic_data_dilemma.pdf

Wetzling, Thorsten and Kilian Vieth-Ditlmann. 2021. *Caught in the Act? An analysis of Germany's new SIGINT reform.* Stiftung Neue Verantwortung. Available at: https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform_0.pdf.

Wetzling, Thorsten. 2020. *Germany's troubled trajectory with mass surveillance and the European search for adequate safeguards*. Policy Paper commissioned by the Israel Public Policy Institute. Available at: https://www.ippi.org.il/germanys-troubled-trajectory-with-mass-surveillance-and-the-european-search-for-safeguards/

Yeh, Chih-Liang. 2018. *Pursuing Consumer Empowerment in the Age of Big Data: A Comprehensive Regulatory Framework for Data Brokers*. Telecommunications Policy Vol. 42, No. 4: 282–92. Available at: https://doi.org/10.1016/j.telpol.2017.12.001

Zegart, Amy B.. 2022. *Spies, Lies, and Algorithms: The history and future of American intelligence.* Princton University Press. Available at: https://press.princeton.edu/books/hardcover/9780691147130/spies-lies-and-algorithms.

Oversight Activity Reports

BfDI - Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. 2021. *Tätigkeitsbericht 2021*. Available at: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/30TB_21.html

BfDI. 2021. *BfDI kritisiert 1.000 Tage ohne Umsetzung von JI-Richtlinie.* Available at: https://www.bfdi.bund.de/SharedDocs /Pressemitteilungen/DE/2021/02_fehlende-Umsetzung-JI-Richtlinie.html

CNCTR - Commission nationale de contrôle des techniques de renseignement. 2021. *6e Rapport d'activité 2021*. Available at: https://data.guardint.org/en/entity/xqss3aic0t9

CTIVD - Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten. 2022. *Automated OSINT: tools en bronnen voor openbronnenonderzoek.* Nr. 74. Available at: https://www.ctivd.nl/ onderzoeken/aivd-mivd-onderzoek-automated-osint

CTIVD. 2017. *Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD*. Available at: https://www.ctivd.nl/documenten/rapporten/2018/02/13/index

EOS Committee. 2020. *Annual Report 2020.* Available at: https://eos-utvalget.no/wp-content/uploads /2021/04/EOS-annual-report-2020-final-version.pdf

IPCO - Investigatory Powers Commissioner's Office. 2020. *Annual Report of the Investigatory Powers Commissioner 2019.* Available at: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf

NSIRA - National Security and Intelligence Review Agency. 2021. *NSIRA 2020 Annual Report.* Canada. ISSN 2563-5778. Available at: https://www.nsira-ossnr.gc.ca/wp-content/uploads/Annual-Report-2020-October-18-2021-FINAL-for-the-Prime-Minister-English-for-printing-1.pdf

PCLOB - Privacy and Civil Liberties Oversight Board . 2022. *FBI Collection of Open-Source Data.* Available at: https://www.pclob.gov/Projects.

TET - Tilsynet med Efterretningstjenesterne. 2022. *Annual report: Danish Defence Intelligence Service.* Available at: https://www.tet.dk/wp-content/uploads/2022/06/FE_UK_2021_web.pdf

Case Law

BGH, Decision of the 31.1.2007 - StB 18/06. *Covert online searches of a computer.* Investigating Judge of the BGH. NStZ 2007, 279. Available at: https://beck-online.beck.de/Bcid/Y-300-Z-NSTZ-B-2007-S-279-N-1

BVerfG, Judgment of the First Senate of 11 March 2008 - 1 BvR 2074/05 -, recital 1-185, http://www.bverfg.de/e/rs20080311_1bvr207405.html

BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07 -, paras. 1-333, http://www.bverfg.de/e/rs20080227_1bvr037007en.html

BVerfG, Judgement of the First Senate of 10 June 2009 - 1 BvR 706/08 -, paras. 1-242, http://www.bverfg.de/e/rs20090610_1bvr070608en.html

BVerfG, Judgment of the First Senate of 2 March 2010 - 1 BvR 256/08 -, paras. 1-345, http://www.bverfg.de/e/rs20100302_1bvr025608en.html

BVerfG, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, recital 1-407, http://www.bverfg.de/e/rs20220426_1bvr161917.html

CJEU. Judgments of the Court (Grand Chamber) of 6 October 2020 Privacy International (C-623/17, EU:C:2020:790) and La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18, EU:C:2020:791)

ECtHR. Malone v. the United Kingdom, application no. 8691/79. Available at: https://hudoc.echr.coe.int/rus

International Regulatory Frameworks

Council of Europe. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Budapest Convention).* 12.05.2022. Available at: https://rm.coe.int/1680a49dab

Council of Europe. *Convention 108+*. 18 May 2018. Available at: https://rm.coe.int/convention-108 -convention-for-the-protection-of-individuals-with-regar/16808b36f1

European Union. *Law Enforcement Directive.* 27 April 2016. Available at: https://eur-lex.europa.eu/ eli/dir/2016/680/oj

European Union. *General Data Protection Regulation.* 27 April 2016. Available at: https://eur-lex. europa.eu/eli/reg/2016/679/oj

Recommended Further Reading

Kans, Michael. 2021. *Data Brokers and National Security*. Available at: https://www.lawfareblog.com/ data-brokers-and-national-security

Office of the High Commissioner for Human Rights. 2022. *Berkeley Protocol on Digital Open Source Investigations.* Available at: https://www.ohchr.org/sites/default/files/2022-04/ OHCHR_BerkeleyProtocol.pdf

Sherman, Justin. 2022. *The Open Data Market and Risks to National Security.* Available at: https://www.lawfareblog.com/open-data-market-and-risks-national-security

About the Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent, non-profit think tank working at the intersection of technology and society. SNV's core method is collaborative policy development, involving experts from government, tech companies, civil society and academia to test and develop analyses with the aim of generating ideas on how governments can positively shape the technological transformation. To guarantee the independence of its work, the organization has adopted a concept of mixed funding sources that include foundations, public funds and corporate donations.

About the authors

Dr. Thorsten Wetzling heads the research unit "Digital Rights, Surveillance and Democracy" of the Stiftung Neue Verantwortung. His current project work focuses on the practice, the legal basis and effective independent oversight in regard to different modes of access and subsequent processing of personal data by security and intelligence agencies. Thorsten directs the European Intelligence Oversight Network (EION) where new ideas and challenges for democratic intelligence governance are being explored in collaborative workshops with oversight practitioners from across the continent. Thorsten is also the founder and chief editor of aboutintel.eu – a European discussion forum on surveillance, technology and democracy. From 2019 to 2022, Thorsten co-directed an international research consortium that has produced, among other things, tools and instruments for future empirical studies in the thematic field of intelligence cooperation and control.

Dr. Thorsten Wetzling
twetzling@stiftung-nv.de

Charlotte Dietrich is a project manager for Digital Rights, Surveillance and Democracy at SNV where she works on strengthening democratic oversight of intelligence services and connecting oversight agencies from all over Europe through the European Intelligence Oversight Network (EION). She also manages the intelligence-oversight.org plattform, an interactive database on international good practices in SIGINT governance. Charlotte holds a Master's degree in National Security Studies from King's College London's Department of War Studies and studied Political Sciences at Sciences Po Paris and the Saint Petersburg State University for her undergraduate studies.

Charlotte Dietrich
cdietrich@stiftung-nv.de

Imprint

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net